Risto Vänni

Emergency preparedness investigation and emergency procedure development for oil industry

Metropolia University of Applied Sciences

Bachelor of Engineering

Chemical Engineering

Thesis

4.2.2016

Tekijä(t) Otsikko Sivumäärä Aika	Risto Vänni Häiriöohjeiden kehittäminen ja häiriöihin varautuminen öljyteollisuudessa 56 sivua + 3 liitettä 4.2.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Kemiantekniikka
Suuntautumisvaihtoehto	
Ohjaaja(t)	Lehtori Timo Seuranen

Prosessien hallinta on monimutkaistunut viime vuosina merkittävästi. Lisäksi erilaiset häiriötilanteet käyvät yhä harvinaisemmiksi. Näistä seikoista johtuen ohjeiden merkitys on lisääntynyt. Tutkimuksen tavoitteena oli tehdä selkoa Porvoon öljynjalostamon käytössä olevaan dokumentointijärjestelmään, prosessinohjaukseen, sekä siihen, miten erilaisiin koko jalostamoa koskeviin häiriöihin on varauduttu. Lisäksi tarkoituksena oli selvittää häiriöohjeiden mahdolliseen kehittämiseen liittyviä perusteita ja tarvetta. Dokumentointijärjestelmää ja prosessinohjausjärjestelmiä tutkitaan yleisellä tasolla. Tämän kaltainen tarkastelu on välttämätöntä työn loppuosan ymmärtämisessä. Koko jalostamoa koskevia häiriöitä tarkasteltiin niiltä osin, kun niihin oli ohjeistuksilla varauduttu ja kartoitettiin oliko joillekin uusille ohjeille tarvetta.

Opinnäytteessä tutkimusotteena on käytetty suunnittelututkimusta (design research). Suunnittelutukimuksen tavoitteisiin kuuluu innovatiivisuus ja tulevaisuuden tarpeisiin keskittyminen pikaoppaiden osalta. Pikaoppaita on tutkittu Porvoon jalostamolla aiemminkin ja tarkoituksena tässä tutkimuksessa oli vertailla erilaisia ohjepohjia sekä kerätä niistä parhaita osia yhteen. Häiriöohjeiden kehittämismallina on käytetty NASA:n tuottamaa suositusta checklist-tyyppisistä ohjeista, jonka tilaajana on ollut Yhdysvaltain viranomainen NTSB. NTSB tutkii lento-, tie- ja rautatieliikenteessä sekä putkistokuljetuksissa tapahtuvia onnettomuuksia ja vaaratilanteita. Mallin avulla voidaan parhaimmillaan määrittää ne asiat, jotka ovat häiriötilanteisiin suunnitellulle pikaoppaalle ominaisia ja sitä kautta kehittää uusi pikaopaspohja häiriötilanteita varten.

Työn tavoitteena on tutkia mahdollisia puutteita tai vaikeaselkoisia kohtia ohjeistuksissa Porvoon jalostamolla. Näiden huomioiden pohjalta on tarkoitus luoda pikaoppaalle malli, jossa on otettu huomioon tieteelliset sekä käytännön kautta opitut perusteet ohjeiden suunnittelussa. Mallin pohjalta on päämääränä luoda pikaopas, jota on mahdollisimman helppo ja nopea käyttää, mutta mallin käyttö vaatii operaattorilta perustietämyksen prosessiyksiköstä.

Avainsanat	häiriö, ohjeet, öljy, jalostamo, pikaopas, checklist, häiriötilanteisiin varautuminen

Author(s) Title Number of Pages Date	Risto Vänni Emergency preparedness investigation and emergency procedure development for oil industry 56 pages + 3 Appendices 4th of February 2016
Degree	Bachelor of Engineering
Degree Programme	Chemical Engineering
Specialisation option	
Instructor(s)	Timo Seuranen, Lecturer

Nowadays process control is becoming more complex, process disturbances are occurring very rarely and the importance of procedures is increasing. This research studies the process procedure system, process control systems, level of preparedness against emergency/process disturbance situations in Neste Oyj, Porvoo refinery.

The second part of this research is designing emergency procedure template for oil industry which utilizes the lessons from Neste's Porvoo refinery, two nuclear power plants in Finland, NASA's contract report 177549&177605 and several other documents that are investigating procedures and all the matters related to procedure design.

The documentation system and the process control systems are studied in general level which is necessary for understanding the rest of the research. Process disturbances concerning the whole refinery are examined only to the extent that are predetermined in the current procedure system.

The research approach was to design science and the goal was to be innovative and to look far into future of procedure designs. Quick reference guides have been designed and studied earlier in the Porvoo refinery as well. The purpose of this thesis was to compare all these designs together and to find all the best parts in them. The checklist template designed by NASA has been used partly as a design model in this research. NASA has produced instructions for making the checklists to National Transportation Safety Board from USA which are used widely in the aviation. At its best, the new model can be used to determine the factors that are typical for emergency quick reference guides. The model is used to develop a new quick reference guide template, which guides the designers to produce reliable quick reference guides.

The aim of the thesis was to inspect possible vulnerabilities in the procedures of Porvoo refinery and to create a template that takes scientific and the lessons from practice into account. The objective is to create a model that is assisting the process operator to give very quick and reliable response to a process disturbance. The model requires that the operator has not less than basic knowledge of the process unit.

Keywords	emergency, procedures, oil, refinery, quick reference guide, checklist, emergency preparedness

Contents

Abbreviations

Neste	Neste Oyj (former Neste Oil Oyj)
NJ	Neste Jacobs Oy
CR	Control Room
HMI	Human Machine Interaction
HRA	Human Reliability Analysis
EEMUA	The Engineering Equipment and Materials Users Association
HAZOP	Hazard and operability study
DCS	Distributed Control System
BV	Bureau Veritas
SIS	Safety Instrumented System
APC	Advanced Process Control
FCOM	Flight Crew Operation Manual (aviation)
OM	Operational Manual (aviation)
QRH	Quick Reference Handbook (aviation)
NNC	Non-Normal Checklist (aviation)
AFM	Aeroplane Flight Manual
EAC	Emergency and Abnormal Checklist
OSBL	Outside of the Battery Limit

BLEVE	Boiling Liquid Expanding Vapor Explosion
NPD	Norwegian Petroleum Directorate
CW	Cooling water
JVL	Cooling water system
BESSI	Gasoline Isomerization unit
HEXI	Isohexane removal unit
NExBTL	Renewable diesel unit
RT3	Crude oil distillation unit
BERP3	Gasoline desulphurization unit
KTO	LPG recovery unit
RET	Distillation unit of platformer
BEHY	Gasoline hydrogenation unit
REF3	Platformer (= Reformation unit)
HEY	Hexane removal unit
VHVI	Very high viscosity index unit
KTVL	Gas turbine power plant
KTY	Gas oil distillation unit
OKSY	Oxygenate removal unit
PELME	Flight petrol sweetening unit

VK	Hydrocracking unit
KAAPO	Gas oil aromatics removal unit
FCC	Fluid catalytic cracking unit
LCF	Lummus Cities Fining
MHC	Mild hydrocracking unit
ATM	Atmospheric distillation unit
VY	Hydrogen unit
VAC	Vacuum distilling unit
CAT	Catalyst treatment unit
PÖY	(LCF, MHC, ATM, VAC, CAT)
ALKY	Alkylation unit
KH	Utilities system
BIY	Bitumen unit
TT2	Vacuum distillation unit
LK2	Thermal cracking unit
KARP	Gas oil desulphurization
SYRP	Gas oil desulphurization
RTO	Sulphur recovery unit
RVTO	Hydrogen sulfide recovery unit

HVY	Sour water unit
NCR	“Neste Continuous improving Reporting”-System
ELY-keskus	Centre for Economic Development, Transport and the Environment
IAEA	International Atomic Energy Agency
STUK	Finnish Radiation and Nuclear Safety Authority

Preface

The author wants to thank everyone involved in this thesis. Thanks to Mr. Asaf Degani, to TVO and to Fortum who gave the author few hours of their time to explain their procedure systems. Special thanks to shift nr. 5 in Porvoo refinery.

The author learned that procedure design needs vast amount of resources from the company and from the personnel. The thesis took more time and energy than the author planned ahead, however, it gave more than it took. There are still many questions unanswered to author. Perhaps there is a subject for the Master degree. Kiitos.

List of Figures and Tables

1 Introduction

This thesis studies the aspects of emergency preparedness at oil refineries generally and uses Neste Oyj Porvoo oil refinery in Finland as an example. Porvoo refinery is a very complex refinery, and it has most of the process units used at modern day refineries; hence it is a great example for the research. The chapter of checklist/quick reference guide development is done with help of Fortum Oyj Loviisa nuclear power plant visit, TVO Olkiluoto nuclear power plant visit and Mr. Asaf Degani formerly from Intelligent Systems Division in NASA.

The first chapters of the research are describing the documentation system, process control systems and alarm systems in Porvoo refinery. The following chapters are describing the fire fighting in oil refineries generally, and Porvoo refinery's preparedness against major disturbances. Final chapters are utilized for developing checklist templates according combined learns from two oil refineries, aviation and nuclear power plant. All previously mentioned items are inspected from emergency preparedness point of view.

The author has witnessed some deficiencies in the documentation during his 8 years as a process operator in two different oil refineries in two European countries. These deficiencies motivated him to seek possible improvements through this research. Most of the deficiencies are usually found in older process units; they are minor safety wise and the reason for them is usually lower standards in documentation in the 60's, 70's and 80's. Process units from the 21st century are usually documented in high standard, and the deficiencies are different. The deficiencies in the 21st century documentation are usually packed around poor typography, impractical templates as well as excessive information to operators.

Although procedures are one of the fundamental pillars of safe industrial process control, it has been difficult to find researches concerning emergency checklist development for oil industry. Unit downtime time costs significant amounts of money, is always a safety hazard and increases equipment malfunctions drastically.

2 Process unit procedure system of Porvoo refinery

The purpose of this chapter is to give the reader a basic knowledge of process unit procedure system design in Porvoo refinery. The chapter does not include any licensor documents or any other documents that are used in the refinery. By reading this chapter, the reader has enough information to understand the following chapters which are describing the procedure systems in Neste's refineries as well as the chapters that are describing the procedure development for oil refineries generally.

Neste follows corporation standards of setting up ID-system for creating documents including unit specific procedures in Porvoo refinery. The management has chosen to use several different main IDs which are separating different departments from each other. For production and logistics the main ID is "OQD-" followed by three to four digits of numbers (some exceptions may exist). The ID-system is being used in Porvoo refinery, Naantali refinery, Singapore refinery, Rotterdam refinery, terminals and research & technology -department. The document ID has to be requested from the administrator of the Corporate Management System (CMS). The ID has a position in the Kameleon document template. OQD-system works in Sharepoint workspace which does not have license fees (Hujanen, 2011).

Finnish law does not require certain kind of procedure management system. However, Neste management system follows several certificates including ISO 9001 and ISO 14001. Additionally, Finnish industrial chemical regulation requires sufficient management system which provides sufficient information and work procedures as well as emergency procedures for the employees (Hujanen, 2015).

Neste's management system is inspected by certifier BV (Bureau Veritas) and TUKES (the Finnish Safety and Chemicals Agency) (Hujanen, 2015).

Every process unit has specific unit folder where all the important procedures are placed. Unit folder structure and minimum amount of information has been approved by TUKES. Every procedure has unique OQD-number, and they are found from physical folders in the control room, field operators' social spaces and production manager of the line's offices. The procedures are found from company's intranet as well. Additionally, there are temporary procedures for abnormal operation situations which are also found from intranet. Plant engineer's responsibility is to make a note to JAWA (e-log book) that there are new temporary procedures to be followed.

Every unit folder in Porvoo refinery follows specific structure: process description, normal operation, start-up procedure, shutdown procedure, emergency procedure, controls and interlocks, safety and used chemicals, catalyst and handling, device procedures, device list, blinding descriptions and other procedures. Only exception is production 4 in Porvoo which has additional information in unit folders (Honkimaa and Ranta, 2011).

Checklists are not officially in the OQD-system, and the checklists are not checked periodically same way as procedures in the OQD-system. However, some lists may exist in the OQD-system as an attachments that should be updated with the correspond OQD-file.

3 Process control systems generally in Porvoo refinery

3.1 General

Chapter 3 gives an overall view of process control systems used in Porvoo refinery. There are also some additional information that describes process control systems in other Neste's refineries. The purpose of this chapter is to give the reader a basic knowledge of automation designs in a modern day refinery which will help the reader to understand the matter on following chapters.

All production lines in Finland as well as in Rotterdam and in Singapore refineries are using Distributed Control Systems (DCS) for controlling the process. Neste uses several different control systems: Metso DNA, Emerson deltaV, Valmet Damatic, Altim Alcont, Ahslström Alcont, Metso, Honeywell Experion PKS and Honeywell Alcont (Arimo, 2013). A list of the process control systems used in the Porvoo refinery is presented in Figure 1.

DCS-system	DCS start-up year	Process unit
Manufacturer 1	1989	JVL
Manufacturer 1	1991/2007	~~KARP3~~/NExBTL1, RL
Manufacturer 1	1993	TANK FARM
Manufacturer 1	1993	RT3, BERP3, KTO4, RET
Manufacturer 2	1993	TRUCK DEPOT
Manufacturer 1	1994	BEHY
Manufacturer 1	1997	REF3, MTBH, HEY
Manufacturer 2	1997	VHM, KTO3, TL1
Manufacturer 1	1998	KTVL3, VL
Manufacturer 1	1999	KTY, OKSY, PELME
Manufacturer 1	2001	VK, VY KAAPO
Manufacturer 1	2001	FCC, KTO3
Manufacturer 3	2003	RAIL CAR UNLOADING
Manufacturer 4	2003/2007/2009	EMU / NExBTL1 PRETREATMENT 1&2
Manufacturer 4	2006	PÖY, VY2
Manufacturer 4	2007	HARBOUR
Manufacturer 1	2008	KH, ALKY
Manufacturer 4	2009	NExBTL2
Manufacturer 4	2009/2010	BIY, TAME, UTILITIES
Manufacturer 4	2010	TT2, LK2, KARP2
Manufacturer 4	2012	SYRP
	2013	BENSIININ VALMISTUS
	2013	SATAMA, VRU
	2013	*KAPR3 (ei vielä käytössä)*

Figure 1. Process control systems in Porvoo (Arimo, 2013)

DCS is used to control the process units by the control room operators. Complex refineries, as Neste Porvoo, requires a vast amount of controllers, automatic valves, measurements and cable work. DCS is a preferred way to control the process because the process control is not bound to happen in one physical location. This means that the process may be controlled elsewhere if the control room is compromised.

3.2 DCS

In the Porvoo refinery the DCS systems are not duplicated. However, often the process stations are duplicated. If the measurement is considered to be critical for the process, the measurement is often duplicated, and the measurements are using different I/O-cards (Arimo, 2013).

Process computers, service stations and alarm stations are duplicated. If one of the stations is malfunctioning it may be replaced with a new station without causing any breaks to stable process control. If one of the I/O-cards of the DCS malfunctions, all the measurements and controls are lost until the card is replaced with a new card (Arimo, 2015).

3.3 SIS

SIS (Safety Instrumented System) is duplicated in Porvoo refinery. SIS works over and without the DCS, see Figure 2. If some part of the process reaches the set-point value of the interlock, the SIS will make an action over the DCS. In interlock situation the operator is unable to control the interlocked part of the process before the cause of the interlock has been removed or the interlock has been bypassed by the instrumentation department.

Interlock and alarm features are important part of process safety. Purpose of these features is to: protect humans, environment and process equipment. Safety automation should be very reliable. Malfunctions in SIS may cause significant damage to people, environment and process equipment (Neste Oyj, 2013).

All the equipment that are related to process safety have to fulfill Finnish laws, regulations and standards. The standards are: IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) and IEC 61511 (Functional safety - Safety instrumented systems for the process industry sector). IEC 61508 is a basic functional safety standard applicable to all kinds of industry and IEC 61511 sets out practices that ensures the safety of an industrial process through the use of instrumentation (such as SIS) (IEC, 2010&2013). See automation hierarchy in Figure 2.

I/O-cards are duplicated in SIS. If one card malfunctions the other shall proceed without any breaks. The malfunctioned card may be removed and replaced with a new one. Central processing units are duplicated as well.

There are few different SIS-systems being used in Porvoo refinery. FSC (Honeywell Alcont), HIMAx (Metso DNA) and relays (Emmerson DeltaV). See Appendix 1 for complete listing.

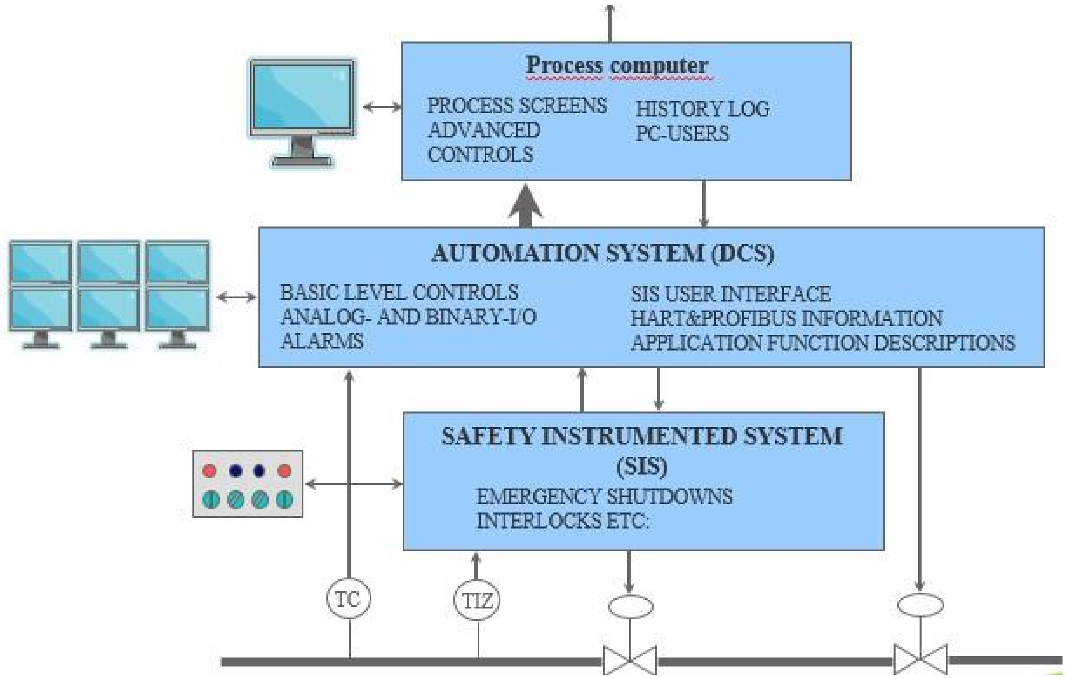


Figure 2. Automation hierarchy in Porvoo (Arimo, 2013)

Neste Porvoo is slowly trying to get rid of the relay logics of SIS for the reason that relays have few unreliability factors. In addition, the relay logics have to be tested manually periodically.

3.4 APC

APC is a model-based multi-variable control system which controls larger process entities. APC may be used to control average reactor bed temperatures for an example. Without APC the DCS could have eight valves to control (in cascade with the bed temperatures) and the bed temperatures would not be as stable as with the APC. This could affect to yield, lifetime of the catalyst and so forth. In addition, the APC can be used to predict fast changes in a process (furnace outlet temperature for an example) and therefore prevents process disturbances (Arimo, 2015).

3.5 PMS

PMS or so called TOP-system is used to gather all the main measurement information for history trending, but it may be used for alarm screening, to control APC and it has many other functions if desired. TOP-system gathers data from all the distributed control systems. In Neste the TOP-system is mainly used for history trending, advanced process control (APC), for office PC-users (unit performance screening for an example) and as an overall process screens, see Figure 3.

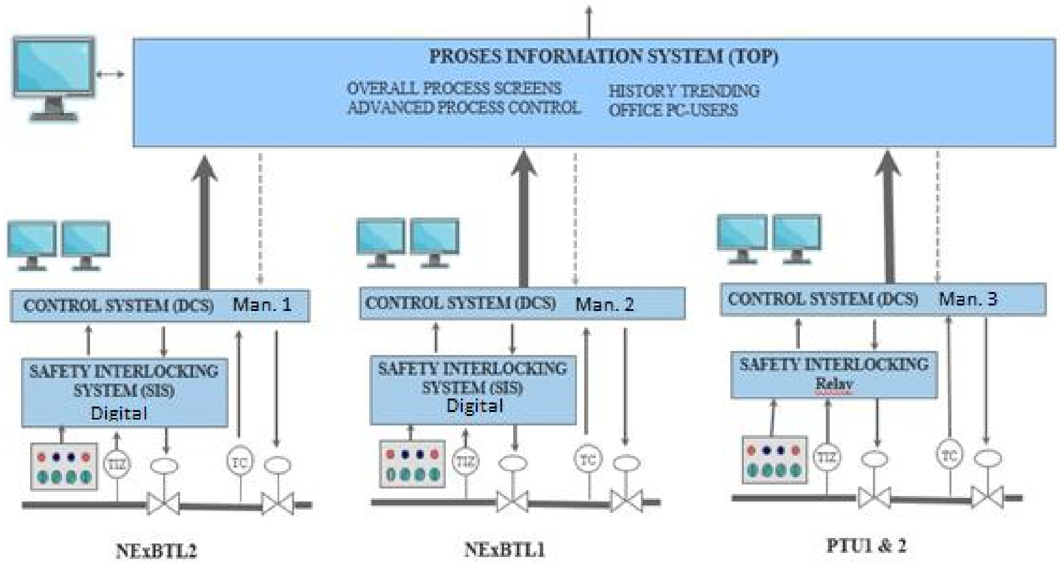


Figure 3. TOP-system in Porvoo (Arimo, 2013)

4 Alarm systems

4.1 General

The purpose of this chapter is to give the reader a basic knowledge of alarm systems, especially with integrated alarm systems in the DCS. By reading this chapter the reader should understand the meaning of alarm systems for processes, the hierarchy of alarms, to understand human capabilities in high load situations, and techniques to reduce alarm flooding during process disturbances.

4.2 General guidelines of alarm systems

Process alarm systems should be developed in line with procedures and process control systems. The aim should be to combine these three fields of knowledge to work smoothly along each other. The target for the developers should be that the systems are consistent and the logic of the systems is the same throughout the refinery (or production lines, assuming that the turnover of operators over the production lines is very low).

The NPD (Norwegian Petroleum Directorate) has revealed unsatisfactory conditions related to alarm systems on oil production sites on the Norwegian continental shelf. The author assumes that same kind of challenges may be discovered all around the world in oil refineries. Alarm system is critical for safe process control; hence the alarm systems should be developed as much as possible. Alarm system should be designed according to recognized principles for human-machine interaction, available human factor and behavior knowledge since the alarm system is vital for safe operation of oil refinery (NDP, 2011).

As the refineries are growing even more complex the HMI becomes more and more important. The design of control systems as well as alarm systems has to recognize human nature and its limitations.

Alarm system should be designed to co-op with the operators, and it should support the operator to concentrate on correct actions and parts of the process unit. This becomes clearer on the process disturbances when the process units are unstable and the alarm system is or should be in major role to support the operator. Risk is that the alarm system stops to support the operator at one point and the volume of the alarms is too high to co-op with. Every alarm should require an operator response. A response could be a physical action to manipulate to process state, to contact field operator or instrument technician or a simple inspection of the process screen (NDP, 2011).

In development state the alarms that are defined by a licensor must always be checked and made sure that they comply with the client’s alarm philosophy (Neste Jacobs, 2014).

Alarm system should be usable in all process conditions and ensuring that unacceptable demands are not placed on operators by exceeding their cognitive capabilities. Alarm rate has to be presented at a rate that allows the operators to understand the purpose of the alarm and to make a correct action.

In an emergency situation the goal state of the plant changes significantly, and the alarm system should be able to adapt to this change. Alarm system should be usable even in the major process disturbances.

As the alarm systems and process control systems are developed the operators should receive training for the basics of the system. Training has to be designed for the needs of operators. Without proper training there is a risk that the alarm systems may be unclear and cause confusion to operators. NPD has concluded a table for maximum alarm rates in disturbance situations in oil refineries, see Table 1.

Table 1: Alarm rates in major disturbances (NDP, 2011)

Alarm rate in major disturbance:	Consequence:
>10 alarms per minute	Excessive and very likely to lead the operator abandoning the use of the system
2-10 per minute	Hard to cope with
<1 per minute	Should be manageable, but may be difficult if several alarms require a complex operator response

The alarm system should be provided with various utility programs, a performance monitoring system for an example. This system should include tools and methods for measuring performance indicators in an alarm system. Information from performance monitoring system is used for continuous improvement of the alarm system. Continuous improvement should lead to improvements with low interval so that the operators are able to adapt to updates. Process simulator, if available, should be used for tuning the performance of the alarm system.

A fault tolerant alarm system ensures that the critical information is always available to the operators, both in normal operation and in an emergency situation. Alarm system should be redundant as well as DCS and all the critical I/O cards, bus systems and CPUs. UPS should be provided for the critical parts of the process, alarm system and process control system for an example.

Alarm systems response time should not exceed over 2 seconds. For presentation in main alarm lists, a time stamping resolution of 1 second will be sufficient. In the alarm log and for use by the suppression logics, 100 millisecond time stamping or better is required. Sometimes it is important to see which caused the disturbance in the unit; hence faster time stamping gives better understanding of start of the problem (NDP, 2011).

Neste has considered pop-up alarm screens for critical alarms, but have chosen not to use them, but instead to decrease the amount of alarms to make it easier to react for the control room operators. V. Kuuluvainen stated that Neste has discussed about alarm sound inhibition timers. The operators could inhibit the alarm sound with a special timer button, which would mute the sound for specific amount of time. Neste chose not to use the system. However, Neste chose a goal to decrease the amount of alarms in disturbance situations as well as in normal operation (Kuuluvainen, 2015).

4.3 Alarm suppression

The objective of alarm suppression is to ensure that the alarms are relevant to the operator's work under the current process conditions and to avoid alarm flooding during process disturbances. Alarm information presented should be important and cause action from the operator. In disturbance situation alarm flooding is always risking the plant and drifting the plant towards interlock state (NPD, 2011).

Control room operators should be familiar with the alarm suppression system, see Figure 4. System should be well documented in understandable way and the system description should be easily found. On a redundant measurements there should be suppression for the measurements in unusual process conditions to reduce amount of alarms from the measurements. For an example, there should be one alarm of equipment shutdown to control room, and all other alarms should be suppressed that are consequences of the equipment shutdown. For an example the suppression activates when the recycle compressor stops and prevents alarm flood from oil pressures, vibrations and low compressor load to operator. This is very useful and has high impact on the task load of the operator.

Alarm suppression should be used prior to alarm filtering. As said the suppression is preventing too many alarms from triggering, but the alarms will be shown on detail pages for further investigation. If the alarms are filtered the details are lost which is not recommended (NDP, 2011).

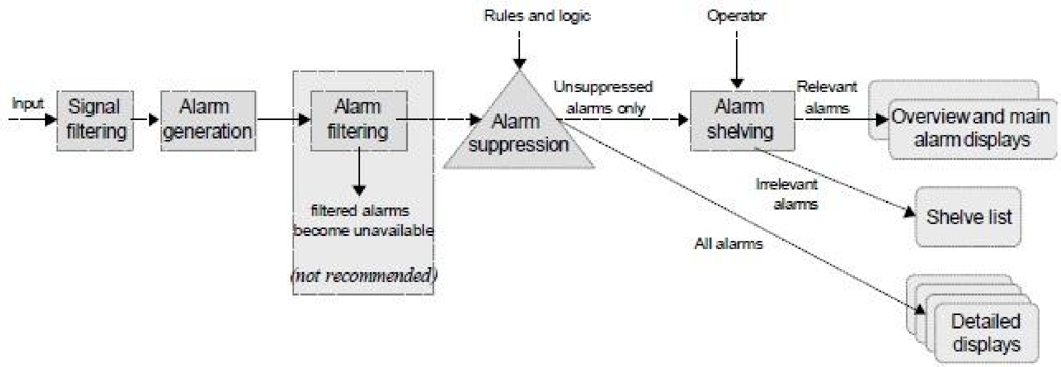


Figure 4. Alarm processing and handling concepts (NDP, 2011)

4.4 Alarm prioritization

Prioritization of alarms is critical for safe control of the process units. Prioritization is used to help the operator to decide which alarm require immediate action and which alarm may wait. All the alarms should be prioritized to different categories. It is not recommended to use more than 4 categories (NDP, 2011).

Commercial airline companies have commonly 4 alarm categories as well. A maximum of three priorities should be used within any one type of display for normal display of alarms. An additional fourth priority level for safety-critical alarms could be used, but these are presented very rarely. The fourth category may also be used to inform ON-state of the equipment once started.

It is important to be consistent with the alarm priority definitions throughout the whole refinery. Changing the priority categories for specific alarms should be done by authorized automation personnel only.

Priorities should be categorized according the severity of the consequences if the operator does not make an action after the alarm has been triggered. When the alarm suppression works properly and the alarms are categorized properly the operator may find the important information quickly from the alarm screen.

There should be relatively small amount of high priority alarms that direct the operator's attention towards the most important alarms, see table 1 (NDP, 2011).

It is recommended to assign alarm priorities based on the target occurrence rate for each priority. In addition, and the most importantly the priorities should be assigned according the vitality of the alarm for the safe and stable plant operation. This priority categorization happens usually naturally for the reason that the vital components for the process are usually chosen and designed to be most reliable parts of the process and the alarm occurrence rate is very low. It is recommended to use three main priority categories. The fourth category may be put aside because the occurrence rate of these alarms should be extremely low or used only as an ON-state alarm. It is recommended that 80% of the alarms should be in the third priority category, 15% should be in the second highest priority, 5% in the first priority category and if the fourth category is being used it should include only few extremely high priority alarms that occur very rarely (NDP, 2011).

4.5 Metso DNA visual alarm prioritization categories

Metso DNA is a new generation DCS and it is widely used in Neste, see Figure 1. Alarms are categorized in 4 categories. 3 out of 4 are main alarm categories and the fourth category is used for deactivated alarms.

Metso's categorization system has many improvements compared to few years older systems as Honeywell Alcont TPA. High end suppression system for an example. Alarm suppression is strongly used in Metso's DCS which is a huge improvement to older systems like Honeywell Alcont TPA.

Visual prioritization categories are designed to help the operator to find the most important information from the alarm scree. However, the triangles are rather small and critical category includes very important alarms which may not be forgotten in case of an emergency. The author claims that the alarm suppression has higher impact on the task load of the operator during a process disturbance than the visual prioritization. Practice has shown that the alarm suppression is very effective for lowering the operator's task load.

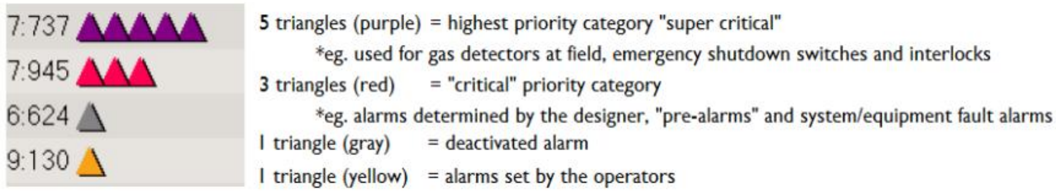


Figure 5. Alarm priorities in Metso DNA in Porvoo (Neste Oyj, 2013)

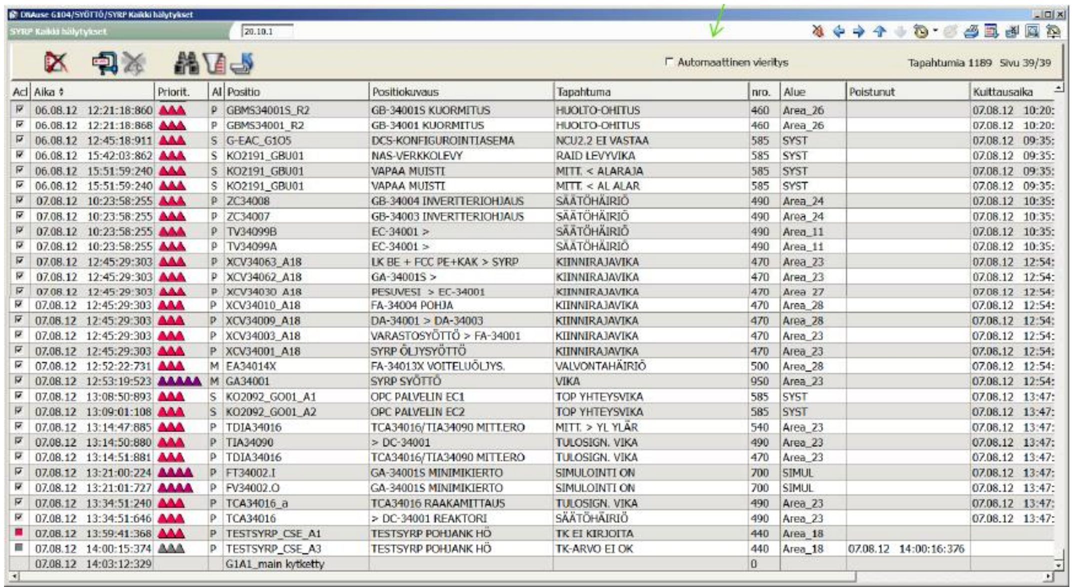


Figure 6. Alarm page in Metso DNA in Porvoo (Neste Oyj, 2015)

4.6 Siemens TXP visual alarm prioritization categories

During the nuclear plant visits the author noticed that the TVO’s plant was using Siemens TXP DCS for turbine side of the plant (Fortum’s representative had PMS for alarm screening and history trending, the rest was analog displays and knobs). Alarm prioritization in TXP was similar to Metso DNA and Honeywell Alcont. There were 3 main categories: Alarm (red A) which was highest in the prioritization category, Warning (yellow W) which was the second in the prioritization category, Fault (F) which was lowest in the main category. It seems that this category system is common in all systems.

4.7 Alarm system development in Porvoo refinery

Present time alarm system, especially Metso DNA, is using automatic masking (or suppression) for alarms. The scope is to reduce the operator's alarm load in unusual process conditions. In addition, some of the alarms are becoming meaningless after equipment has stopped by the operator (Neste Jacobs, 2013).

CR1251 is applied to the projects that are executed by the Neste Jacobs. Alarm system includes "Process alarm" and "Operator alarm". Process alarm has fixed limit that is defined during the design phase. This limit can be changed by authorized personnel only. Operator alarm can be set by an operator and it does not have fixed limits. The alarms that are set by the operators are always lowest priority alarms. The importance of the alarm is determined by the process designer. Neste has acknowledged that the alarm current to operator is considered too high in unusual process conditions (Neste Jacobs, 2013).

On the other hand in HAZOP new alarms are being added to the system. Usually these alarms are in high category and they cannot be suppressed automatically.

Decreasing the operator's alarm load during a process disturbance means a review of the process protections at the end of the basic design phase or at the early stage of execution phase. The review is done to eliminate alarms that become unnecessary after a process protection function, even if they are in the first priority category. This is part of prioritization logic of the alarms.

Alarm masking system has to be reviewed carefully and usually the review meeting includes experts from many departments: process design engineer(s), automation design engineer(s), plant operation engineer(s), experienced operator(s) and others that are considered to be needed for the review.

Unit's most recent PI diagram revision, Safety Integrity Level specification document, cause and effects diagram, HAZOP record and related list of actions should be handed over for the participants of the review (Neste Jacobs, 2013).

5 Emergency management in Porvoo refinery

5.1 General

The purpose of this chapter is to give the reader a basic knowledge of the expenses and the reasons of emergencies, obligations of the personnel during the emergencies and information channeling during the emergencies.

Note that there are many kind of factors that may lead the process to disturbance. Data collected by the Hydrocarbon Publishing Company (HPC) in 2013 shows that there were 1200 refinery shutdowns in the US from 2009 to 2012 in total. 46% of the shutdowns were due to mechanical failures, 19% were caused by electrical disturbances, 23% were result of predetermined maintenance shutdowns and the least 12% were mostly due leakages and process fires (Hydrocarbon Publishing Company, 2013).

Looking at the percentages in Figure 7, it is easy to notice that highest risk for the disturbances are the mechanical equipment (mostly rotary equipment). Electrical disturbances are including shutdowns due bad weather.

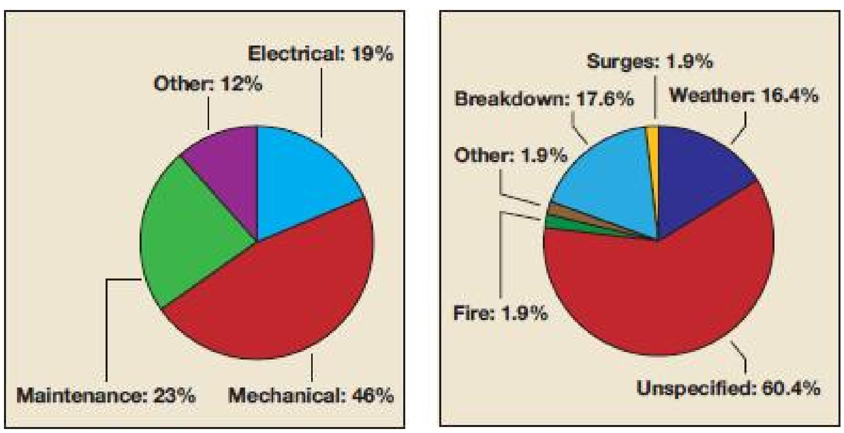


Figure 7. Reasons of shutdowns in the USA and the causes of power disturbances (HPC, 2013)

Main causes to power disturbances are unspecified in their data (60.4%). The reason for unspecific data may be that the refinery did not know the exact reason of the failure while writing the report. Weather was the cause in 16.4% of the cases, breakdowns 17.6% and rest were fires (1.9%), surges (1.9%) and other (1.9%). Weather's high percentage may be explained by the strong storms in the US.

Usually the disturbances are local and not affecting the whole refinery or there are alternative feed sources and production locations in case of process disturbance in one process unit.

This chapter is dedicated for the extremely rare and challenging disturbances that would affect the whole oil refinery or in worst case to shut it down temporarily.

5.2 Announcements and obligations

There are many type of emergencies in oil refineries: process disturbances, process fires, emissions to environment, nuisance or harm to environment and to neighbors, hazards to personnel working in the area and accidents which may lead to injuries or even worse: death.

Neste Porvoo uses information channels depending of the quality, the magnitude and the severity of the emergency. The eye witness is always obligated to inform the product manager of the line and/or control room operator immediately after the accident or other abnormal situation.

If the emergency is not causing unusual noise, process fire, emission, excessive flaring (over an hour), smell, accident, major process disturbance or other major deviation from normal operation the emergency is informed to fire department's "quiet phone number" (if needed) which does not cause a voice alarm system to trigger in the fire department. This kind of situation would be a minor wound to hand of a victim.

If the situation includes any of the previously mentioned items the emergency call out to fire department shall be made immediately. In addition, the refinery's shift supervisor shall be informed by the production manager of the line, if necessary.

Shift supervisor makes actions depending of the emergency. If the emergency happens during normal office hours and includes unusual noise, process fire, emission, excessive flaring (over an hour), smell or a process disturbance the shift supervisor calls to head of supervision and to head of operation department. Head of supervision or head of operation department takes contact to communication manager who makes a deviation report in Crisis Commander (software), to info-phone and to company's deviation webpage. If the emergency includes environmental point of view the environmental manager is included to the process. The info-phone and the webpage are designed to notify neighbor companies and residents about the deviations. In addition, a NCR-report is saved to a system.

If the emergency happens outside of the normal office hours and includes unusual noise, emission, process fire, excessive flaring (over an hour), smell or a process disturbance the shift supervisor makes a deviation report in Crisis Commander by himself. Shift supervisor should never make estimates of production losses in the report. Shift supervisor always decides if he should call to head of supervision or any other manager outside of the normal office hours. In addition, a NCR-report is saved to a system.

In case of a major emergency (severe injuries, death, major fire, major emissions etc.) an emergency preparedness group is been set up. For major emergencies there is an emergency preparedness group: situation director, supervisor of the operations department, a person who is in charge of communication, a person in charge of maintenance, a person from HSSE (personnel safety, work permitting, waste management etc.), corresponding person of the situation information (two persons) and the chief of fire department. In addition, a NCR-report is saved to a system (Neste Oyj, 2015).

The production manager of the line orders the control room operator to turn and lock the surveillance camera to a point at the scene of the incident if possible. Footage from all the cameras is recorded on a digital recorder for later retrieval for investigation purposes (Neste Oyj, 2015).

6 Controlling the Porvoo refinery in a major disturbances

6.1 General

Chapter 6 describes the precautions done by Neste against major process disturbances in a whole Neste's Porvoo refinery area. The author's target is to find the preparedness level of Porvoo refinery against major process disturbances and/or emergencies. Second target is to find possible vulnerabilities and to find a solution and/or recommendations for further investigations.

6.1.1 Steam disturbance

Usually the situation management for steam shortages comes from Porvoo's power plant. This kind of situation may occur when one or more boilers in the power plant shuts down. If the outage is major the shift supervisor starts to manage the steam usage and production in the refinery according the OQD-1547.

In steam shortage the power plant maximizes the production, channel burners are started at KTVL2&3 and opens both transfer lines to production. Production has 4 stage plan against steam shortages.

In the first stage the production of steam boilers are maximized in the production, steam to refinery's edge areas is minimized (see OQD-1547 attachment 1), RVTO3 decreases steam intake, SYRP and KARP2 reduces stripping steam, ADIP circulation is decreased in RVTO1&2, RT3 minimizes steam to preheater EA-10168 and TAME-unit is set to re-cycle. Total estimated saving is 135 t/h of 16bar steam and 46 t/h of 5 bar steam.

In the second stage the KTO5 unit is shutdown, production line 4 switches steam turbine pumps to electrical pumps, FCC decreases steam to BEJT and ALKY minimizes the steam at DA-9801. Total estimated saving is 12 t/h of 5 bar steam, 54 t/h of 40 bar steam and 16 t/h of 16 bar steam.

In the third stage the HEY unit is shutdown, MTBE unit is shutdown, KARP2 is set to recycle, steam usage of HVY4&5 is minimized and stripping steam of TT2 and BIY is minimized. Total estimated saving is 75 t/h of 5 bar steam.

In the fourth stage the RET unit is shut down.

It is very important to maintain at least 14 bar of pressure in the 16 bar steam system. It is important to reduce usage of 16 bar steam which helps the power plant to maintain high pressure on 100 bar system. If the 100 bar system is also loosing pressure the recycle compressors in REF3 has to be shut down which means high production losses (Neste Oyj, 2010).

6.1.2 Power disturbance

Depending of scale and magnitude of the power failure, the electrical duty officer is normally prioritizing the tasks inside the refinery.

Every substation is equipped with an alarm system. All the common alarms are connected to the remote operating systems. In addition, the substations alarm systems are connected to a main power plant's control room. Control room operator is consulting the shift electrician about the alarms.

The refinery's electric network has been protected with relays. When one part of the network is disturbed the relays are automatically protecting the healthy network. The relay system is designed to remove as less as possible of equipment from the network no matter where the disturbance happens (Neste Oyj, 2012).

Porvoo refinery has been equipped with back-up generator system. This system gives power to vital parts of the process when the main power has been lost. It is good to understand that full blackout in Kilpilahti-area is happening very unlikely because the refinery is using the national power grid.

Some parts of the process are equipped with backup power (UPS and diesel generators): the process control systems are equipped with UPS and the UPS are getting power from diesel generators once started. The generators are feeding power to only some predetermined process equipment that are vital for safe shutdown of the refinery.

The diesel generators are starting automatically when the power is lost in the substation (all transformers). Note that the generator tries to start three times automatically in 30 seconds. If the generator fails to start automatically it has to be started manually by the electrician. The generators are used only when the substations is in complete blackout. There are backup transformers for each substation and even if the substation is not equipped with the backup transformer, there are two transformers feeding two separate rails and one transformer can handle two rails.

In local power disturbances (transformer feed cable failure for an example) the system is switching the back-up transformer on automatically (or connecting the healthy transformer to both rails). Feed transfer produces short, few second long blackout. Those equipment that are equipped with automatic restart system shall start automatically in time sequence (to reduce the load of the transformer). There are usually 3 to 4 sequences in 30 seconds.

Diesel generators are started only when there is total blackout in the substations (all transformers are lost). The diesel generators are feeding all the equipment mentioned in the attachment and in addition: the emergency lightning, UPS rechargers, fire alarm systems, fire water system and many other vital systems that need to work in any condition (Järvinen, 2015).

Power failures are usually local, but they are occurring more often than one could presume. From 2009 to 2012 there were 323 refinery or partly shutdowns in the US (Hydrocarbon Publishing Company, 2013).

6.1.3 Hydrogen disturbance

In case of hydrogen shortage in the refinery, some of the process units have to be set to lower feed rater, to recycle or even to complete shutdown. In the night time the shift supervisor is giving orders that which units have to lower their feed rates and how much. In the daytime the production planners are giving orders to shift supervisor which is giving orders to control room and field operators as well as production managers of the line.

Porvoo refinery's hydrogen network is complex and the proper actions have to be discussed with production planners (daytime). Usually if there is shortage of hydrogen the hydrogen units 1 and/or 2 are maximizing their feed rates and try to compensate the loss of hydrogen in the refinery's hydrogen network. Especially when losing the reformatting unit 3's side product hydrogen it is hard for the old compressors to withstand the high hydrogen content in the gas. Detailed description may be found from OQD-2257 (Neste Oyj, 2015).

6.1.4 Instrument air disturbance

If the instrument air pressure is dropping abnormally there are steps to avoid further problems. All the steps are explained in OQD-1553. It is possible to start extra air compressors and if that is not possible, there are valves that connect production lines air systems together. If the pressure is still sinking it is possible to get extra air from the main power plant.

If all the actions have been made and the air pressure is lost due a big leakage for an example, all the unit operators are starting to shut down the units while following the procedures (most of the units are already down because of the S.I.S). After the emergency shutdown it is important to monitor for leakages and to minimize losses (process equipment, health and environment).

Starting up the refinery after a major instrument air failure takes time and the utility systems have to be started prior to process units. Specific unit start-up order has been made and it may be found from OQD-1553 (Neste Oyj, 2015). Note that this order may differ from the procedure OQD-1553 depending of the severity of after effects of emergency shutdowns.

6.1.5 Natural gas feed disturbance

Natural gas (NG) feed is very important for the refinery. NG (=methane) is used to keep the furnaces, turbines and boilers running and the refinery's hydrogen plants are relying on the NG feed for the reformation process.

There are 5 stages of measures to be taken against NG shortage. In stage one all the minor effecting actions are done which reduces NG intake approximately 30 tons/h. In stage 2 gas turbine power plant 3 is stopped and the feed is changed from NG to fuel oil which reduces NG intake approximately 15 tons/h. In stage 3 the hydrogen plant 2 is stopped and the feed gas is changed to propane which reduces NG intake approximately

33 tons/h. In stage 4 which is total NG outage all the rest of the locations that are normally using NG are replaced by fuel gas, propane and/or fuel oil (Neste Oyj, 2015).

If the NG shortage would turn to full cut off it is possible to run Porvoo refinery (to some extinction) with propane, but it has never been tested with the current unit setup. It is possible that not all the process units could be in production if the NG intake would have to be fully cut off. There are plans and procedures made for this situation (Shift supervisor, 2015).

6.1.6 Cooling water disturbance (production lines 1/2/4)

Production line 3 is left out from the research because production line 3 is using separate cooling water system.

If the disturbance is considered as minor (one pump stops and cannot be started for an example) the spare pump is being started. If there is no spare pump available the CW return temperature has to be monitored carefully. If the temperature is not manageable the biggest cooling water users have to be adjusted as needed. KTY in production line 1 is a massive CW user (feed rate of the unit has to be lowered/other process changes made etc.). Depending of the scale of disturbance the other units have to be shutdown/put on recycle.

If the whole cooling water system stops for a short moment it is important to maintain good start-up conditions in CW-system. In this case the process units have to set to recycle or shutdown as long as the CW is unavailable.

If the whole cooling water system stops for a longer period in the winter time, all possible actions to prevent freezing has to be made in addition to stopping the units (Neste Oyj, 2012).

6.1.7 Flare system disturbance

If the process control PCs in the control room are compromised, the controllers are maintaining the current position. TOP-system may be used to monitor state of the process. However, if the disturbance is caused by the bus failure, the TOP-system is unavailable as well. In this case the process has to be monitored at the field (especially the state of the compressors and the liquid levels of the flare drums).

If the problem occurs in the process stations all the valves are set to failsafe state (fail-safe states are presented in OQD-1099).

When the process control has been lost completely the field operators must check that the compressors are stopped, to maintain pilots on at the flares tips and the flare drum levels must be visible.

In case of a total power failure the aim is to maintain pilots on at the flare tips and flare drum levels must be kept visible. Some of the flare drum pumps are connected to diesel generators, exception to this are the well pumps (whole list presented in OQD-1099). If the process control is still on (connected to UPS) the control room operator has to check that the pumps has been started and the drum levels are in control (Neste Oyj, 2003).

6.1.8 Sulphur recovery unit disturbance

Finnish “Environmental Permit” requires that the sulphur recovery rate and the utilization rate of the sulphur recovery units have to reach certain degree. The sulphur emissions has to be decreased to lowest possible level.

Usual reasons for sulphur recovery unit (RTO) disturbances are: sour gas feed quality fluctuations, hydrocarbons in the feed, cutbacks in utilities and equipment failures.

Oil refinery is obligated to inform the ELY-keskus (Centre for Economic Development, Transport and the Environment) in case of a disturbance in the sulphur recovery unit(s). Refinery’s shift supervisor is obligated to inform the environmental manager about the disturbance. Environmental manager makes a notification in the Crisis Commander and a NCR notification (Neste internal system). Environmental manager makes an additional notification to Porvoo’s city hall and the ELY-keskus. Environmental manager updates info-phone (or the shift supervisor in the night shift) and website for the neighbors in addition. These information channels are used to keep neighbor companies and inhab-itants aware of the disturbances.

Disturbance notification is made if: sour gases from one sulphur recovery unit are sent to flare for an hour or more and the instant shut-off valve XCV-7351 is in closed position, sour gases from two or more Sulphur recovery units are sent to flare and instant shut-off valve XCV-7351 is in closed position. If the XCV-7351 is in open position, the flare gases are fed to flare gas recovery unit and then compressed to fuel gas (through the hydrogen sulfide absorber).

If one of the sulphur recovery unit is disturbed the sour gases are fed to other sulphur recovery units. If the gas flow is too high to these units, the Superclaus-reactors may be bypassed. If there is flow of sulphur to flare system, instant actions has to be done. The load of the sulphur recovery units have to be lowered. The load is lowered by means of: lowering the feed rate of the HVY5, HVY5 to complete recycle, lowering the feed rate of the HVY4, HVY4 to complete recycle, KARP3 to minimum feed (feed from tank U-1 maximized) or to complete recycle, SYRP to minimum feed rate or to complete recycle, MHC feed to lower sulphur content, VK to minimum feed rate, NExBTL1&2 to minimum feed rate and by setting the lower sulphur content crude oil tank (cavern type) to recycle. OQD-6802 describes the information channels in detail.

7 Fire fighting in Porvoo refinery

7.1 General notes

The purpose of this chapter is to give the reader a basic knowledge of fire fighting tactics in Porvoo refinery as well as to describe the responsibilities of the personnel.

The actions against process fire are always dependent of scale, location and material of combustion. There are vast amount different sorts of hydrocarbons, gases, chemicals and other combustible material around the oil refinery which brings special challenges against process fires.

7.2 Production department’s responsibilities and tactics against industrial fires

The main responsibilities of production department are: to rescue those in immediate danger and to give first aid, to alert fire-brigade, to start first line fire-extinguishing and to start those operative actions that are required to stop the fire. Those operative actions are: to inform others and evacuate persons that are not required to stay near the location of fire, to shut down the flow of flammable liquid/gas to location of fire, to emergency shutdown the process unit(s) if required (may cause further problems, normal shutdown or recycle state if possible), to release the pressure from the unit if considered necessary, to monitor unit's state continually to notice possible changes in the process equipment (cracks, increasing pressure and so forth), to monitor nearby units (shutdown if necessary) and to maintain normal operation on the units that are not affected by the fire (Neste Oyj, 2015).

7.3 Fire department's responsibilities and tactics against industrial fires

The main goals for the fire department are: to figure out the best and safest driving route to destination, to be located on the safe side of the wind, to inform security guards of area of isolation, to give call out of danger by public address system, to ensure that no one is injured and to ensure that no one is threatened by the fire, to examine that what kind of material is leaking, pressure of the system, temperature of the system (with from production department), to examine if it is possible that the fire may spread to surroundings and to inspect if the other process equipment or structures are compromised, to extinguish the fire quickly (exception to gas leakages, look below), to start cooling down the surrounding equipment and structures with water spray and to inform waste water treatment plant if the foam is being used (Neste Oyj, 2015).

7.4 Extinguishing industrial fires

7.4.1 Flammable gases

If the gas has been leaking for a certain period of time, it may have been gathered as a cloud and when the cloud of gas ignites it will give short “swoosh” sound. The flame front shall proceed from the edges of the cloud through the cloud with speed less than 20 m/s. Radius of hemispherical shaped gas cloud doubles after ignition and after the material has burned to the end the flame proceeds as a pointed flame from the leak source. Pointed flame may ignite immediately or after the swoosh effect. The pointed flame may burn at up to 1300 degrees of Celsius (when hydrocarbons).

Reaction speed at gas cloud explosions might exceed the speed of sound and the pressure wave may cause severe damage. The space where the explosions takes place has significant impact on the severity of the pressure wave. If the space is confined the damages are significantly larger.

BLEVE is an explosion caused by the rupture of a vessel containing a pressurized liquid above its boiling point.

If the gas leakage takes place, but does not ignite there is a significant risk of explosion. If the leakage is considered as large, always evacuate the area. Considering the leaking material it may be recommended to spread the gas cloud with water spray or by using a water wall to prevent the cloud to proceed next to an ignition source (for an example a furnace) (Neste Oyj, 2015).

Generally there are three different options to extinguish a gas fire:

Confining the leakage if possible. Closing valves that will shut off the gas flow to location of the leakage. If the valve is not remotely operable and the valve is located in or near the gas cloud, water spray may be used to confine the gas outside of the valve. Note that the person (if not a fire fighter) who operates the valve should use proper clothing and equipment while operating the valve.

Controlling the flame until the flammable gas flow eventually stops. This manner requires that the nearby structures and equipment are cooled down and the flame is controllable inside the water spray(s).

Extinguishing the flame and closing the source of the leakage. This manner is last option and shall be used only when the flame causes a bigger risk than the gas cloud itself. When using this technique all the preparations against reignition shall be done.

Cooling down the vessel has few basic key points: use fixed water sprays, 10 liters of water per minute per square meter (pointed flame 2000 liters of water per minute) or 100 liters per minute per vessels height meter, spray uniform film of water to the surface of the vessel and make sure there is constant water spray on the vessel (Neste Oyj, 2015).

7.4.2 Flammable liquids

Liquids that have boiling point of 35 degrees of Celsius or lower and flash point of 0 degrees of Celsius are considered as an extremely flammable liquid. Liquids that have flash point of 21 degrees of Celsius or lower are considered as a highly flammable liquids. Liquids that have flash point over 21 degrees of Celsius but lower than 55 degrees of Celsius are considered as a flammable liquid.

In oil refineries the liquids are processed in different kind of pressures and temperatures. Temperature of the substance has an effect on flammability, gasification and on the swoosh effect if the gas cloud is ignited. In the process area the liquid may be in high pressure or the flame may heat up a vessel where the liquid is over its boiling point. These factors have to be considered at all times.

Liquid fires are extinguished with a water spray or with a foam depending of the situation. Structures may be cooled down with a direct water spray or with a water mist. If direct water spray is used it is recommended to collide the spray to object nearby. Colliding the water to an object makes a nozzle effect and the spray is spread in larger area and the cooling is more uniform.

For red-hot metal objects it is recommended to start with a water mist and the mist should cover most of the surface at once. Start with low amount of water and increase the flow in function of time. It is also possible to use rain-technique where the water is sprayed a top of the object and it rains over the object. This technique is particularly recommended for extremely hot objects (furnaces and heat exchangers for an example). Rain-technique prevents too fast temperature shifts which may cause even more severe leakages.

If the leakage is bursting out with pressure the foam is not recommended to be used. The pressure shall push the foam away from the fire. However, the foam may be used for underlying spaces. Water spray and powder is recommended for high pressure leakages.

If the fire is shower (or fountain)-type it is recommended to consider if it is better to let it burn and to control the flames instead. Extinguishing happens through production department (depressurization and draining the equipment). If the flame continues burning more than 5-20 minutes (depending of the situation and location) and there is no consistent water spray, it is recommended to evacuate the area and shutdown the unit(s) from the control room.

In case of a fire on the ground floor it is recommended to use foam even if the sewer system works well. If the sewer system cannot withstand the amount of leaking product or plugs the foam layer will prevent the flammable liquid from flowing to other process units.

Note that it is fire department's responsibility to prevent after effects of a fire and the fire-department shall monitor the location for the required period of time (Neste Oyj, 2015).

8 The design of emergency procedures

8.1 General

The purpose of this chapter is to start a scientific research of emergency procedure development in oil refineries and to find the path for better procedure development. This research tries to combine technical information, theory behind previous procedure designs, to combine knowledge from nuclear power, oil industry and airline industry as well as to find a path for better emergency procedure designs, especially for oil industry.

As discussed in the previous chapters the operation manuals (emergency procedures are usually part of it) are usually heavy to read and are not practical to be used during the process disturbances. Checklists or other practical documentation should always be provided to operators when the process unit is complex, the unit may cause severe damage to other units, hazards to personnel, hazards to environment and/or economical risks to the company. Usually every process unit is at least in one of these group.

Note that the checklist and other documentation should never go past the operator's and/or his supervisor's judgement and the documentation should always be considered as a tool, not as a book of orders. Sometimes it is more important to control the process than to read the checklist. In some situations the operator may find way to maintain the unit in production instead of shutting down the unit. This is wise also in safety point of view (may cause less temperature shifts and equipment shut downs in the unit). However, if the operator feels uncomfortable the checklist or other documentation may calm the person down and point the goal state of the unit.

8.2 Fundamentals of the checklist development

It is highly recommended to have checklists or other practical documentation for unusual process conditions in the oil refineries. Usually all the process units are set to recycle if there is a minor process disturbance. In a recycle state the unit's product(s) is (usually) fed back to the feed drum. Recycle state is usually one of the safest states for the unit in an unusual process condition. It is very important that the operators are familiar of setting the unit to recycle safely and maintaining the unit on recycle for certain amount of time. Note that the safe state may be something else as well.

In some major unit disturbances the aim is to release pressure and flammable material from the unit as quickly as possible, but in a safe manner. These situations are usually called as emergency situations because there is a high threshold to start these actions. In these cases the recycle state is usually not the target state and the operators should be trained and guided by the procedures to know how to act correctly in specific situation. There are usually high amount of process equipment in the process unit and it is not possible (or even convenient) to make emergency procedures to cover all the possible equipment failures. Usually the first impact of the equipment failure targets to one part of the process and this knowledge should be used in favor when developing the emergency procedures and checklists. Note that the previous comment is always depending on the emergency procedure design and cultural habit.

The emergency procedures and checklists should cover all the main parts of the process and their disturbances (loss of cooling water, loss of power, loss of recycle compressor for an example). It should be mandatory to provide sufficient emergency procedures to operators as well as checklists against predetermined process disturbances.

Immediate shutdowns (emergency depressurization for an example) are usually causing equipment failures for the reason that the equipment are getting shocks from fast temperature shifts. The most common failures for this kind of shutdowns are heat exchanger leakages which might emerge to severe process fires.

The checklists could lessen the stress of the operators and to help them know that everything shall be fine when they follow the predetermined steps of the checklist.

8.3 Basic development principles

The function of the emergency checklists or block charts is to ensure that the operators will operate the process units in a satisfactory level in case of a process disturbance. These checklists are used rarely, thus it is very important that the operators are self-studying the emergency procedures and checklists occasionally. It is very important for the operators not to get into situation where they have never been. The meaning of the previous sentence is that the operator should have already thought what happens when different parts of the process are failing.

It should be mandatory to organize toolboxes and brainstorming sessions within the shifts to examine and discuss about the accidents and near misses inside and outside of the company.

8.4 Procedure system in commercial airplanes

It is necessary to do distinction between emergency procedure and emergency checklist. Let us take a glimpse to this subject through the aviation. In aviation you have Quick Reference Handbook (QRH) and Aeroplane Flight Manual (AFM). Quick Reference Handbook contains extracts from Aeroplane Flight Manual. Quick Reference Handbook is often used as an alternative name for Emergency and Abnormal Checklist (EAC). Earlier mentioned Non-Normal Checklist (NNC) is part of QRH. To make the terms a little bit more complicated the AFM is a synonym for Operational Manual (OM). The terms can be quite challenging to a person who is not familiar with aviation, but the basic idea is that you have one Operational Manual which includes all technical data of the aircraft and the QRH includes extracts from the OM. So in theory the OM is used for studying or when the QRH does not provide sufficient information to solve the problem. OM is not practical to use in abnormal situation and for this given reason there is QRH. This system has many advantages: the QRH may be used to set the aircraft in a safe state without forgetting important steps. When the aircraft is in safe state there is time to obtain the

OM and use it to solve the problem (if required). The QRH makes sure that the pilot does not forget these important steps when there is lot of confusion, noise, fatigue or any other distractions that might lead the pilot to forget steps or to do something that is not supposed to do. These tips or learns could be applied to oil industry as well.

8.5 Procedure development notes by NASA

NASA mentions a specific risk of checklists which is easily occurring when the companies are trying to maintain discipline. In some cases the checklist becomes a dumping site to resolve discipline problems or to show management that a specific problem is solved. By solving problems this way the immediate problems may be resolved, but at the same time the importance of the procedures and/or checklists by the operators is reduced which might lead to even more severe problems in the future (NASA, 1990).

8.5.1 Lessons that could be applied in the oil refinery

The emergency checklist or other document should reveal the operator that what are the main tasks to reach safe state of the unit. Note that the safe state might differ depending on the situation. This procedure should be available and obtainable at all times in vicinity of the operator (not in the unit folder or randomly lying on a desk). Procedures should include all the vital items that are needed to be done before the unit is in safe state. Usually this requires separate procedures for control room and for field operator. Procedures should be designed that way that the operators with less work experience would be able to use them if/when needed.

The emergency procedure and the checklist or block chart should be available next to unit’s panel in the control room. Both of them should be easily noticeable and the key points should be found quickly. All the predetermined major disturbances shall be mentioned in the folder separately. There should be assigned responsible person who maintains and updates these procedures and checklists.

8.6 Emergency procedure development in Loviisa nuclear power plant

Figure 8 shows the basic principle of the procedure development system in Loviisa nuclear power plant (originally from Areva). Fortum Oyj started a procedure development and update project in 2004 which is still working in the year 2015. There has been significant changes in the procedure template. Fortum developed the new template with Areva (French multinational group specialized in nuclear and renewable energy), IAEA, STUK on some other partners like Westinghouse. Fortum chose to use block chart type system for emergency procedures to decrease the amount of pages, to make clear path system between procedures and to make parallel actions possible. The block chart template is originally designed by Areva. Operational procedures are still usually as text-type with tables and numbering. Fortum was able to reduce the amount of pages significantly with block chart templates.

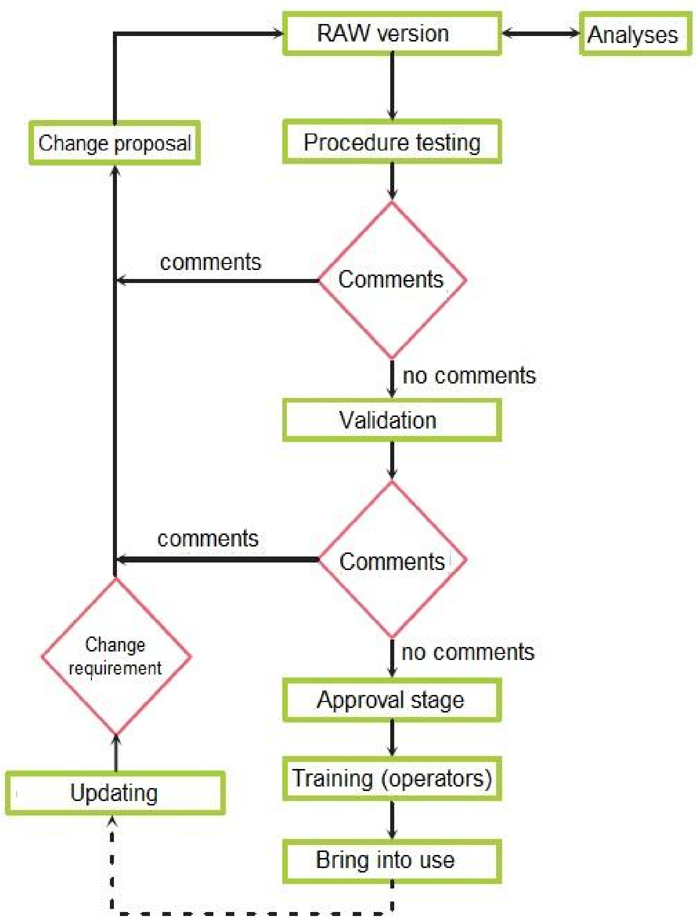


Figure 8. Procedure development system (Fortum Oyj, 2014)

Original procedures were conservative step to step text-type procedures where shift leader was giving orders to the operators. The manuals were really heavy and they were not found practical in Loviisa which was one of the reasons that the project started. Some of the tasks during emergencies or even in minor disturbances were happening in parallel which is challenging to show in text-type procedures.

Fortum's former text-type emergency procedures were quite close to OQD-system in Porvoo refinery. There were some exceptions: the items to be done were placed in tables, numbered and the template was slightly more systematic.

Fortum introduced block chart type procedures to fire fightning procedures as well. Formerly these procedures were also in text-type template which was hard to use in practice. Block chart type procedure gave clear instructions to every department whose obligation is to do what and when. With the new template system the responsibilities became clearer, it was easier to see parallel actions during the drills, it was easier to lead the situation and the system was clarifying the responsibilities and tasks against after effects.

Fortum was using identification procedures to identify specific risks. These procedures were used to follow the correct procedures in specific process states. The procedures were also guiding the operator (or shift leader) to change the procedure if specific points are reached in the process (reactor pressure decreases significantly for example).

All the items in the new procedure design are predetermined and they have boundary conditions (maximum temperature for an example). These conditions include and may withstand certain amount of additional problems happening in the process. However, if these boundaries are exceeded the block charts are telling the reader to change to higher risk category. This category means that the situation has become more threatening and bigger actions have to be done to prevent catastrophic failures.

There were many similarities that could be used in favor for designing the procedures for oil industry (most of them are listed in the end of the research). It has to be mentioned that the power plants process seems to be slightly slower (or it has been designed that way) than many oil refinery's units. The procedure system is really heavy and high in detail. It could not be used directly in the oil refinery. However, there were many properties that could be used (high end block chart template design for an example).

8.7 Typography

The object of this part is to bridge the gap between the basic knowledge of typography and the personnel that are designing the checklists for oil industry.

There are many types of documents employed in the control room. There may be typographical deficiencies as well as outdated data that has not been removed.

There are vast amount of aspects when designing the checklists. The report focuses on typographical factors such as typefaces, character height, use of lower- and upper-case characters, line length, and spacing. Some graphical aspects such as layout, color coding, fonts and character contrast are also discussed.

There was little information in literature for typography in emergency checklists. Therefore, the information in this research is based on field studies done by the author. Different kind of templates are found in subchapter “Checklist template comparison”.

When specifying the graphical appearance of checklists the designer must be careful in combining several non-optimal conditions. These combinations tend to reduce the overall efficiency of the checklist (NASA, 1992).

Author recommends using “List of Design Recommendations” from “On the typography flight-deck documentation”, Asaf Degani, 1992 for designing checklists for oil refineries.

As stated by Mr. Degani it is not simple to produce checklists that all the possible readers would perceive the information accurately. It is highly possible that it is impossible to produce this kind of checklists. However, designers should get closer to perfection by means of typography. These learnings may be used while designing the emergency checklists for the oil refineries.

8.7.1 Readability

Text should be written such way that a single word, word-groups, abbreviations and symbols could be easily recognized from the text. This means that the spacing of individual characters, spacing of words, spacing of lines and the ratio between character area and the background (NASA, 1992).

8.7.2 Reading conditions

Reading conditions may change over a day and seasons. If the emergency checklist is being used in the field, there might be very moist, rainy, windy or snowy which are making reading very difficult. If the lights are dim in the control room during night time it affects optimal reading conditions negatively (NASA, 1992). Do not use gray text over white background for this reason. Always print on water-proof paper for field use. See figure 9 for letterforms.

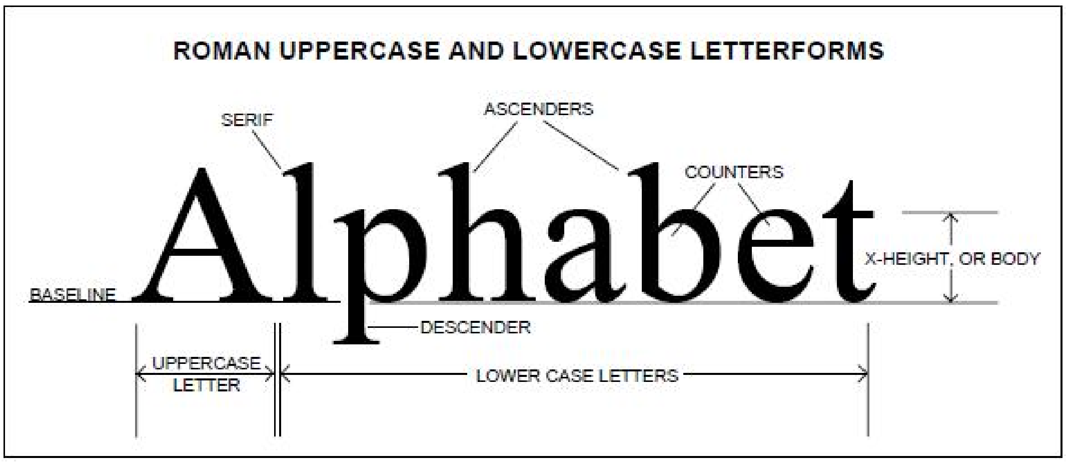


Figure 9. Letterforms and names (Degani, 1992)

8.7.3 Fonts

Fonts refer to alphanumeric style used in printing. There are thousands of fonts available for different uses. Aviation industry uses mainly two fonts for checklists: roman and sans-serif. Roman is mainly used in newspapers, journals and books. Sans-serif is a modern font that does not include the little strokes that project horizontally from the top or bottom of a main stroke (NASA, 1992).

Mr. Degani states that several researches have reported that sans-serif fonts are more legible than roman. He also states that the thought behind this is that the sans-serif letters are simpler and clean (NASA, 1992).

Serifs may add uneven appearance to the strokes and shapes. However, they make reading more fluent and help the eyes to follow to horizontal movement. For this given reason it is important to use adequate spacing between the letters while using sans-serif instead of serif font. The designer has to be aware of this to prevent eyes from skipping a line while reading the emergency checklist. Avoid using long strings of text set in italics and use primarily one or two fonts for emphasis.

There are many different fonts in the sans-serif group. In checklists it is important to use characters that are not similar to each other, O and C for an example. Most modern sans-serif fonts are having too much similar fonts and should not be used for this given reason. Sources of similarity between the characters of modern sans-serif fonts as follows: appearance of the letters “P” and “R”, the effect of mirror images between the upper and lower part of the letters (“E”, “B”, “D”), the use of equal radius for different letters (“G”, “O”, “C”).

8.7.4 Lower-case and upper-case characters

Several research are stating that the lower-case characters are more legible than upper-case characters (Hartley, 1981; Philips, 1979; Tinker, 1963). Poulton (1967) performed an experiment to determine the difference in a reader’s attention between upper and lower-case in newspaper headings. He reported that the lower case headings were located faster than upper case heading. Tinker (1963) tested lowercase and upper-case fonts for legibility and pleasantness. He reported that lower case was read faster and ranked higher in pleasantness (NASA, 1992).

Lower-case characters are the most used in everyday life and this might be one of the reason that the upper-case characters are harder to read. Another factor is that the lower-case characters are spread further away from each other which helps eyes to recognize them better (NASA, 1992, p.12).

A shape of a familiar word is stored in the memory. While reading text the brains are matching the observed word and the remembered memory patterns. Therefore, when the word patterns are easily recognized by the brain it is easier to match the observed words to memory patterns; hence reading becomes faster, pleasing and more accurate (NASA, 1992, p.13).

Research (Philips, 1979) has shown that the emphasis given to the first letter of a word will improve the speed of search. This finding is legit for lower-case as well as upper-case words. Most of the flight-deck documentation and aviation checklists used today are set in upper-case (NASA, 1992).

8.7.5 Horizontal and vertical spacing of the characters

Horizontal and vertical spacing affects the readability of the text especially when the font height is small. The recommended vertical space between lines is 25-33 percent of the overall size of the font (Tinker, 1963; Woodson, 1981). The horizontal space between characters is recommended to be approximately 25 percent of the overall height and not less than one stroke width (NASA, 1992, p.13). See figure 10 for optimal spacing.

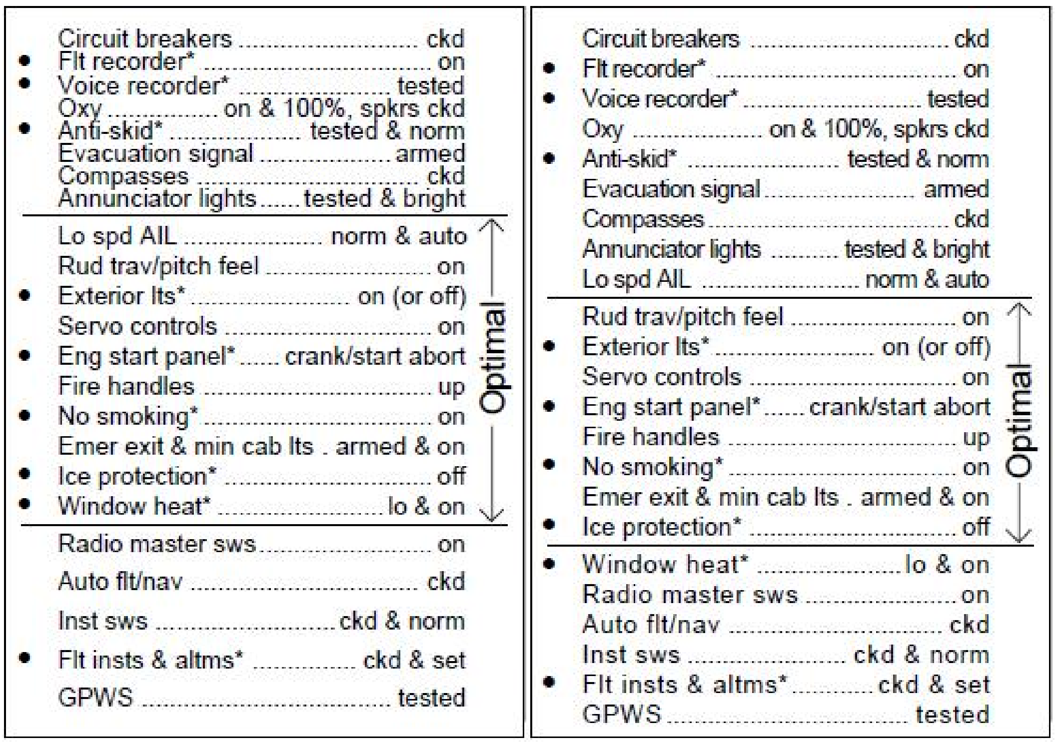


Figure 10. Optimal vertical and horizontal spacing (NASA, 1990)

8.7.6 Color coding

Some airlines use color coding to make distinction to normal checklists, abnormal checklists and emergency checklists. Black print over white is used for normal checklists, black over yellow is used for abnormal checklists and black over light red is used for the emergency checklists. For better color contrast yellow over black and blue over white are recommended choices (NASA, 1992, p.23).

8.7.7 Cognitive limitations

Effects of cognitive task load are highly dependent on task duration. Usually the negative effects of the task load are increasing over time, see figure 11.

	Task Performance Period		
	Short (<5min)	Medium (5-20min)	Long (>20min)
Time occupied *Low* Info processing *Low* Task switches *Low*	no problem	Under-load	
Time occupied *High* Info processing *Low* Task switches *Low*	no problem		Vigilance
Time occupied *High* Info processing *All* Task switches *High*	Cognitive lock-up		
Time occupied *High* Info processing *High* Task switches *High*	Overload		

Figure 11. Task load over time (Mark A. Neerincx, 2003)

Vigilance is a problematic factor for operators which may cause problems to concentrate. Vigilance increases when there is low task load, but time occupied is long. Performance decrease can already occur after 10 minutes when an operator has to monitor a process continuously, but does not have to act. Vigilance may cause stress, but it may also cause boredom which leads to lower stage of alertness. In high risk plants this is always a safety risk (Levine et al., 1973; Parasuraman, 1986).

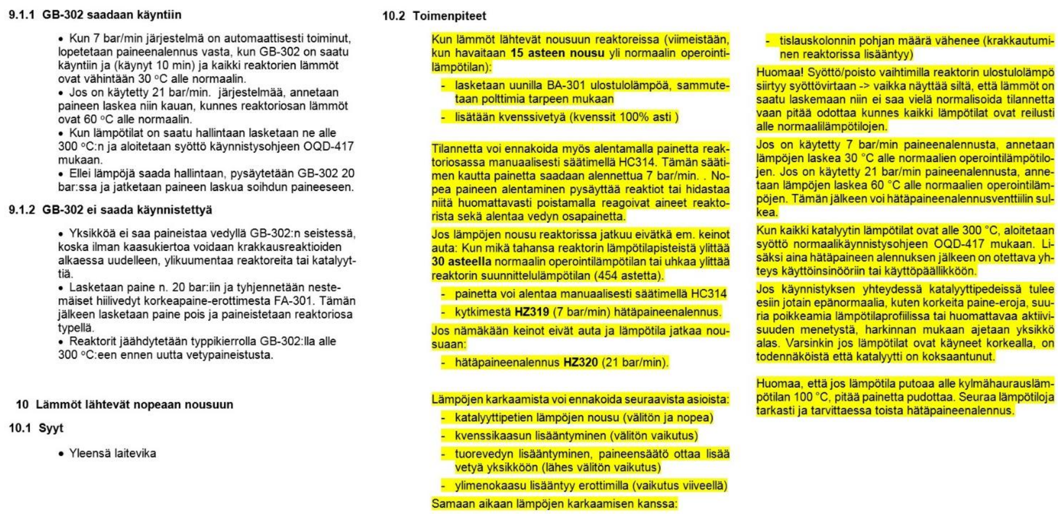
Humans are inclined to focus on one task and are unwilling to switch to another task even when the second task has a higher priority. They are stuck to their choice to perform a specific task (Boehne & Paese, 2000).

There is a possibility that checklists could decrease the effect of the vigilance and minimize the effect of inclined focus. Step-to-step system guides the operator to follow the "guided route" to a safe state of the plant. This should be acknowledged by the company's management (Mark A. Neerincx, 2003).

Considering the previous chapters it is recommended to use checklists at least in the high risk units to reduce task load and to minimize the effects of vigilance or overload.

8.8 Checklist template comparison

Procedure template of Figure 12 follows chronological order. Procedure explains possible reasons for the disturbance and then lists the correct actions to be taken. In typography point of view the text is written clearly, however, some of the procedures are providing high amount of information which may confuse the reader especially during the process disturbance. Some of the letters are packing up which is not recommended.



9.1.1 GB-302 saadaan käyntiin

- Kun 7 bar/min järjestelmä on automaattisesti toiminut, lopetetaan paineenalennus vasta, kun GB-302 on saatu käyntiin ja (käynyt 10 min) ja kaikki reaktorien lämmöt ovat vähintään 30 °C alle normaalin.
- Jos on käytetty 21 bar/min. järjestelmää, annetaan paineen laskea niin kauan, kunnes reaktoriosan lämmöt ovat 60 °C alle normaalin.
- Kun lämpötilat on saatu hallintaan lasketaan ne alle 300 °C:n ja aloitetaan syöttö käynnistysohjeen OQD-417 mukaan.
- Ellei lämpöjä saada hallintaan, pysäytetään GB-302 20 bar:ssa ja jatketaan paineen laskua soihdun paineeseen.

9.1.2 GB-302 ei saada käynnistettyä

- Yksikköä ei saa paineistaa vedyllä GB-302:n seistessä, koska ilman kaasukiertoa voidaan krakkausreaktioiden alkaessa uudelleen, ylikuumentaa reaktoreita tai katalyyttiä.
- Lasketaan paine n. 20 bar:iin ja tyhjennetään nestemäiset hiilivedyt korkeapaine-erottimesta FA-301. Tämän jälkeen lasketaan paine pois ja paineistetaan reaktoriosa typellä.
- Reaktorit jäähdytetään typpikierrolla GB-302:lla alle 300 °C:een ennen uutta vetypaineistusta.

10 Lämmöt lähtevät nopeaan nousuun

10.1 Syyt

- Yleensä laitevika

10.2 Toimenpiteet

Kun lämmöt lähtevät nousuun reaktoreissa (viimeistään, kun havaitaan **15 asteen nousu** yli normaalin operointilämpötilan):

- lasketaan uunilla BA-301 ulostulolämpöä, sammutetaan polttimia tarpeen mukaan
- lisätään kvenssivetyä (kvenssit 100% asti)

Tilannetta voi ennakoida myös alentamalla painetta reaktoriosassa manuaalisesti säätimellä HC314. Tämän säätimen kautta painetta saadaan alennettua 7 bar/min. . Nopea paineen alentaminen pysäyttää reaktiot tai hidastaa niitä huomattavasti poistamalla reagoivat aineet reaktorista sekä alentaa vedyn osapainetta.

Jos lämpöjen nousu reaktorissa jatkuu eivätkä em. keinot auta: Kun mikä tahansa reaktorin lämpötilapisteistä ylittää **30 asteella** normaalin operointilämpötilan tai uhkaa ylittää reaktorin suunnittelulämpötilan (454 astetta).

- painetta voi alentaa manuaalisesti säätimellä HC314
- kytkimestä **HZ319** (7 bar/min) hätäpaineenalennus.

Jos nämäkään keinot eivät auta ja lämpötila jatkaa nousuaan:

- hätäpaineenalennus **HZ320** (21 bar/min).

Lämpöjen karkaamista voi ennakoida seuraavista asioista:

- katalyyttipetien lämpöjen nousu (välitön ja nopea)
- kvenssikaasun lisääntyminen (välitön vaikutus)
- tuorevedyn lisääntyminen, paineensäätö ottaa lisää vetyä yksikköön (lähes välitön vaikutus)
- ylimenokaasu lisääntyy erottimilla (vaikutus viiveellä)

Samaan aikaan lämpöjen karkaamisen kanssa:

- tislauskolonnin pohjan määrä vähenee (krakkautuminen reaktorissa lisääntyy)

Huomaa! Syöttö/poisto vaihtimilla reaktorin ulostulolämpö siirtyy syöttövirtaan -> vaikka näyttää siltä, että lämmöt on saatu laskemaan niin ei saa vielä normalisoida tilannetta vaan pitää odottaa kunnes kaikki lämpötilat ovat reilusti alle normaalilämpötilojen.

Jos on käytetty 7 bar/min paineenalennusta, annetaan lämpöjen laskea 30 °C alle normaalien operointilämpötilojen. Jos on käytetty 21 bar/min paineenalennusta, annetaan lämpöjen laskea 60 °C alle normaalien operointilämpöjen. Tämän jälkeen voi hätäpaineenalennusventtiilin sulkea.

Kun kaikki katalyytin lämpötilat ovat alle 300 °C, aloitetaan syöttö normaalikäynnistysohjeen OQD-417 mukaan. Lisäksi aina hätäpaineen alennuksen jälkeen on otettava yhteys käyttöinsinööriin tai käyttöpäällikköön.

Jos käynnistyksen yhteydessä katalyyttipedeissä tulee esiin jotain epänormaalia, kuten korkeita paine-eroja, suuria poikkeamia lämpötilaprofiilissa tai huomattavaa aktiivisuuden menetystä, harkinnan mukaan ajetaan yksikkö alas. Varsinkin jos lämpötilat ovat käyneet korkealla, on todennäköistä että katalyytti on koksaantunut.

Huomaa, että jos lämpötila putoaa alle kylmähauraslämpötilan 100 °C, pitää painetta pudottaa. Seuraa lämpötiloja tarkasti ja tarvittaessa toista hätäpaineenalennus.

Figure 12. Emergency procedure in OQD-system (Neste Oyj, 2010)

Weakness of this system is that the predetermined major disturbances are not presented clearly in the unit folder. Disturbances are not clearly placed disturbance per page. In addition, the text follows book-like order which is challenging to use in practice.

This system is useful for self-studying and it can explain actions and other information in detail. For this reason it appears to be very effective system if it is regularly used for self-studying and the emergency checklists are designed to work in same logical order with this detailed description. The author considers the OQD-system to work the same for oil industry as an Aeroplane Flight Manual for aviation. Note that the emergency procedures should be kept up to date with the checklists. Font is Arial size 11 which is easy to read and could be considered as one of the best options for this kind of procedure.

Note that it is recommended to have separate folders for the operational manuals and emergency procedures. In the OQD-system the emergency procedures are placed in the unit folder which is not practical for the operators.

Checklist style of Figure 13 lists few main predetermined disturbances for the process unit. Column on the most right corner lists the main disturbances. When the current disturbance has been found the reader may follow the row to the right. On the top row are the items to be taken in consideration in logical order (from left to right). On the row which the current disturbance exists, are the actions to be taken.

Fortum
Oil and Gas
Porvoon jalostamo/
J Koskinen

TOIMINTAJÄRJESTELMÄ
Operointiohje
25.2.2004

OQD-1059
VERSIO 7
28 (28)

VHVI-YKSIKÖN HÄIRIÖTILANTEET, YHTEENVETO TOIMENPITEISTÄ

TOIMENPIDE / HÄIRIÖ	Hätäseis HZ36062	BA-36001 1)	Tuorevety PCA36015	Syöttö 6) FCA36003	Reaktoriosan paine 3) PIA36008	Kvenssit ja kaasukierto	TCA36101:n ohjaus 2)	FA-36003:n pinta 4) LCA36003	Vesisyöttö FCA36012	Tislausosa
Reaktorilämpötilojen karkaaminen	Odota	Pysäytä	Pysäytä	Maksimoi	Alenna (HZ-36049)	Maksimoi	100 %	Valvo	Pysäytä	Pitkä kierto 7)
GB-36001 pysähtyy	Odota	Lukitus	Pysäytä	Maksimoi	Alenna (HZ-36049)	Katkeaa	100 %	Valvo	Pysäytä	Pitkä kierto 7)
Sähkökatko	Käynnistä	Lukitus	Lukitus	Lukitus	Laskee 700kPa/min	Katkeaa	100 %	Valvo	Lukitus	Seis
Syöttö katkeaa	Ei	Lukitus	Vähennä 5)	Seis	Ylläpidä	Lisää	100 %	Valvo	Pysäytä	Lyhyt kierto
Tuorevety katkeaa	Ei	Tehoa alas	Seis	Seis	Laskee	Ylläpidä	100 %	Valvo	Ylläpidä	Pitkä kierto 7)
Tuorevety vähenee	Ei	Tehoa alas	Häiriö	Vähennä	Ylläpidä	Ylläpidä	Ylläpidä	Valvo	Ylläpidä	Ylläpidä
Pohjapumput	Ei	Lukitus	Vähennä 5)	Pysäytä	Ylläpidä	Maksimoi	Ylläpidä	Valvo	Pysäytä	Ylläpidä
Kuumaöljykierto	Ei	Tehoa alas	Vähennä 5)	Vähennä	Ylläpidä	Ylläpidä	Ylläpidä	Valvo	Ylläpidä	Pitkä kierto 7)

1) Kaikissa häiriöissä vähennä tehoa tai pysäytä uuni, alenna ulostulolämpöä 55 'C:tta. Lopeta jäähdytys, kun häiriö on ohi.
2) Kun TCA-36101:n ohjaus (ulostulo) on 100 %, ohittuvat lämmönsiirtimet ja jäähdytys on maksimissaan.
3) Kun paine on laskenut alle 5 Mpa (50 bar), lopeta paineenlasku ja katkaise syöttö.
4) Painenalennustilanteessa varaudu avaamaan toinen LCA-36003 (A tai B) kentältä
5) Jos lämmöt reaktoreissa lähtevät nousemaan, katkaise tuorevetysyöttö

Syötön sisäänottolämpötilat (minimi): DC-36001 **300 'C**
DC-36002 **200 'C**

6) Pysäytä GA-36001, jos imulämpötila (TIA36003) nousee yli **180 'C**

7) Linjaa DA-36003:n pohjaöljy EA-36014:n kautta syöttösäiliöön ja katkaise raskassyöttö. Lopeta prosessiöljyn ulosotto.

Figure 13. Table-style emergency checklist for VHVI-unit (Neste Oyj, 2004)

Once the reader knows how to read the template it is quick to use and takes only few seconds for the reader to determine the correct actions for the situation.

Downside of the system is the large size of it. If the process unit has high amount of predetermined disturbances and high amount of actions to be taken the table may become illegible. Another downside is that if the emergencies have high variety of the items the aspect of the table changes considerably and the template is not consistent. The reader have to be very careful for not jumping over the items and the template gives very general information to reader. Some notes are added to bottom of the template and navigating through the template is very challenging. The template is too technical in practice.

In Figure 14 is a typical checklist of an airplane. The item to be checked or configured is placed on the left column. Dot line connects the item to the action. Many items and actions are written in abbreviations. Checklists are read from top to bottom which is the correct logical order for the current situation.

BEFORE STARTING ENGINES

	CIRCUIT BREAKERS	CKD
•	FLT RECORDER*	ON
•	VOICE RECORDER*	TESTED
	OXY	ON & 100%, SPKRS CKD
•	ANTI-SKID*	TESTED & NORM
	EVACUATION SIGNAL	ARMED
	COMPASSES	CKD
	ANNUNCIATOR LIGHTS	TESTED & BRIGHT
	LO SPD AIL	NORM & AUTO
	RUD TRAV/PITCH FEEL	ON
•	EXTERIOR LTS*	ON (OR OFF)
	SERVO CONTROLS	ON
•	ENG START PANEL*	CRANK/START ABORT
	FIRE HANDLES	up
•	NO SMOKING*	ON
	EMER EXIT & MIN CAB LTS	ARMED & ON
•	ICE PROTECTION*	OFF
•	WINDOW HEAT*	LO & ON
	RADIO MASTER SWS	ON
	AUTO FLT/NAV	CKD
	INST SWS	CKD & NORM
•	FLT INSTS & ALTMS*	CKD & SET
	GPWS	TESTED
•	ENG INST/N_1 COMPUTER*	CKD & TESTED
•	GEAR LEVER*	DN, 3 GREEN
	OMEGA*	CKD
	FLAP/SLAT LEVER	W/GAGES
	SPEED BRAKES	RETRACT/DISARMED
	FUEL LEVERS	OFF
•	PK BRKS & PRESS*	SET & CKD
•	RADAR & TRNSPDR*	STBY
•	TRIM CONTROLS*	SET
	MAN DEPRESS VLV	CLOSED
•	ELEC PANEL*	CKD & SET
•	BATTERIES*	NORM
	FUEL PANEL	CKD & SET
•	FUEL QUANTITY*	___ LBS, CTRS RESET
•	HYD PANEL*	CKD & SET
	OIL QUANTITY*	___ QTS
•	APU*	CKD
	FIRE & SMOKE DETECTION	TESTED
•	AIR COND & PRESS*	CKD & SET
•	RAM AIR INLET SWITCH*	NORM CLOSE
•	VENT PNL*	CKD/BLOWER OFF
	TEST PANEL	NORM & OFF
	PROBE HEAT	CKD & OFF

Figure 14. Typical checklist in aviation (NASA, 1990)

Downside of this system is the high amount of abbreviations. However, the risk of misunderstandings may be lowered considerably by training. Also the dot line may guide the reader to wrong action, especially when the line is long.

The amount of the items does not change the appearance of the template considerably. System may be used during the emergency situation as well as normal start-up or shut-down situations.

This list type may not be used directly in oil refinery because there is not enough room for the text. However, there are items that could be used for the checklist. These items could be the dot line which could be used to reach uniform template which does not change drastically if the sentences are different in length, which typically is the situation. Another item is the stacking of items underneath each other. However, in the refinery there are usually many actions happening along each other. This may lead to a risk that the operator follows one step too cautiously and does not read the following step which may be already in higher priority. The risk could be decreased by proper training, but not removed completely. System to decrease this risk should be inspected.

Figure 15 presents high amount of information in one page. Checklist includes nearly as much information as the OQD-template in Figure 12. The difference is that the template lists only the items to be done. The template does not explain the possible causes for the disturbance.

NESTE OIL

20: NExBTL, Set-up list, field operator

Done:	*Feed cut to 20DC-01; unit to circulation:*
	Open 20DA-02 stripping steam to atm. (when steam XCV to 20DA-02 is closed). Close steam hand valve to 20DA-02.
	Line 20GA-26/S discharge up to 20DC-02 with 20MV-1032 (+2 MVs at the 20EA-06A). Ctrl. flow with pump's discharge (if/when needed).
	Check that the MV to rerun bullet is open and close MV to storage (consult panel man).
	Close 20FA-05 gases to ejector (20FA-45) at 20FA-08 tower.
	Membrane package/20PK-04 (stop/start both trains online): o Close inlet chain valve. o Close permeate outlet hand valve (after 20HV-800). o Release pressure from permeate side to flare (before 20HV-800). o Make N2 connection. Open all automatic valves from permeate side (except 20HV-800). o Start purging through permeate (H2) side to flare.
	Open 20FA-22/S (20GB-02/S suction volume bottle drainage) to flare slightly (to drain possible liquids).
	Make nitrogen connection to 20DA-04A/B inlet and start purging.
	Line 20DA-06 bottom back to 20FA-15 instead of WWT.
	20GA-16/S: set stroke to 0%, stop the pump and close one discharge valve.
	Make nitrogen connection to 20FA-05 water boot (when needed).
	Check 20EC-01 and Hot Oil exchangers for leakages.
	Check vulnerable locations for leakages.
	Stop 20GA-01/S when temperature rises at the 20FA-01 and feed will be out for a while.
	Close analyzer valves if/when required (especially recycle gas).
	Additional info:
	20DA-03 by-pass (20FA-02 gas phase directly to 20FA-09 through 20EC-04) valve 20MV-1872 may be opened when gas recycle at the 20DC-01 is required, but sour gas absorbing is not desired.
	Line up the steam from the header to 20EA-22 and 20EA-35 (when 20EA-09 doesn't produce steam anymore). Open 20MV-1472 from the steam header (20DC-02 tower, behind 20FA-18). Close valve after set-up! (+ normal checks).
	20GB-01 trip: start compressor e-driven frame lube oil pump running and stop it when compressor is running. Make sure that lubricator is on "Auto"-mode and check that it works well after start-up. (+normal checks).
	20GB-03 trip: close CW to 20EA-47A/B to reach start-up condition temperature, start electric frame lube oil pump, press "Trip reset", start lubricator and start compressor. After start-up make sure that e-driven frame lube oil pump is stopped and CW is opened back for 20EA-47A/B.

Neste Oil Netherlands B.V.

Figure 15. Unofficial checklist template of Neste oil (Neste Oyj, 2012)

Downside of this template is the enormous amount of text. It may take too long for the control room operator to follow this checklist to be usable. The template is also inconsistent.

This kind of checklist could be used in normal start-up and shut-down situations. Operators should have enough time to read it during these process conditions and the amount of information should be increased for these occasions (compared to disturbances).

Figure 16 represents a checklist with more visual aspect. It is drawn with block charts. Orange color block is the start of the disturbance. Operator checks the folder for the occurred problem and then starts to follow the correct checklist from the top to down. Blue blocks are presenting possible causes and ways to fix the problem. Yellow diamond shaped blocks are question blocks that are questioning the operator if the problem was fixed. After yellow blocks the operator may answer to the question and follow the correct path.

Downside of this system is the multiform aspect which may lead the operator to confusion. More practical research is needed for this system to become standard template. Block charts have huge benefit on steps that should happen in parallel. Any text-type system lacks this prospect. When the items may be displayed in parallel it helps the operator to concentrate on all the items happening at the same time. Text-type system lacks this parallel feature and it may lead the vigilance to decrease towards other events in the unit.

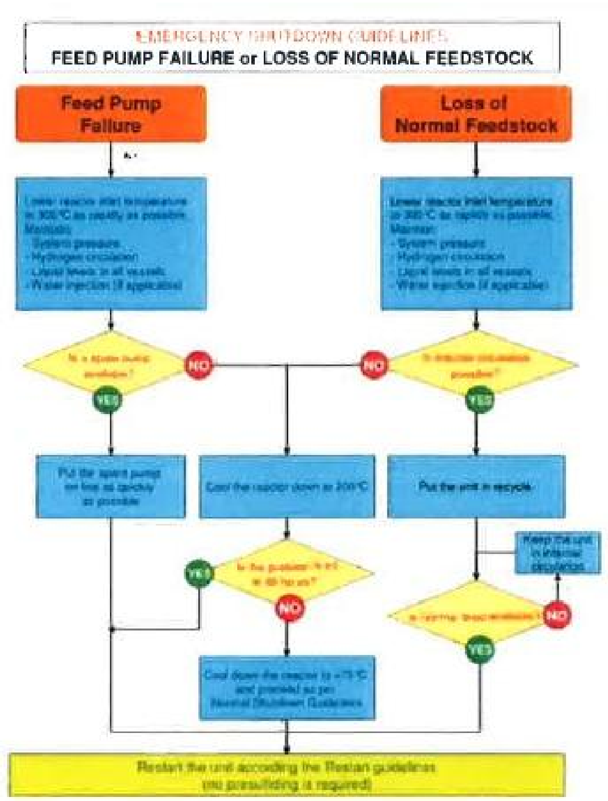


Figure 16. Block chart type emergency checklist (Albemarle Catalyst Academy, 2010)

Figure 17 presents an official checklist design used in production line 4 in Porvoo refinery. Control room operators in production line 4 recommended the checklist system to be used in normal shutdowns and start-ups. They have found it useful.

Production line 4 is the newest production line in Porvoo refinery which is started in the 21st century. In typography point of view the system is using sans serif font Arial, size 12. The vertical spacing between the lines is 2 which is considered large, however, the items in the checklist are pleasurable to read. The items are placed in their own rows separated with the bullet marks. Checklist is not providing very detailed information, it is only listing the key points in the emergency. This system has proved benefits for the operators. This system has excessive amount text and information that could possibly be reduced in order to make the list even easier to read.

NESTE OIL **Cutback lyhennelmä**

Versio 1

ESD-71122 Hätäpaineenalennus

- **Kytkin → HZ-71024A**

LCF-osa

- Hätäpaineenalennus (Yksikön paine → 35bar)
- Maakaasua 7,3 t/h. 12 min.viive. 10min. rampilla
- Älä ohita tarpeellisia lukituksia
- Vuodon sijainnin ja määrän perusteella päätetään syötön katkaisusta, eristetään vuoto mahdollisuuksien mukaan
- Paineenalennuksen jälkeen pysäytetään toinen tuorevetykompressori GB71001A/B/S (cutback toiminto)
- Lopetetaan maakaasun syöttö GB71001A/B/S:lle ja liitetään typpispooli imuun ja siirrytään typpiajolle jos tilanne vaatii typetyksen.
- OSBL KART/LCF KART → FA-71001 (vaihto ½ tunnin kuluessa)
- EBU-pumppujen kierrokset → 700 rpm. (cutback-toiminto)
- Varmista, että reaktori on öljytäytössä ennen kuin nostat EBU-pumpun kierroksia.
- Jos katalyyttipeti on romahtanut, vetyä ei saa ottaa takaisin reaktoriin ennen kuin lämmöt alle 390 °C ja leijunta on palautunut normaaliksi (Huom. vetysäätimien asennot)
- Tarkastetaan, että automaattiset cutback toiminnot ovat menneet läpi
- Tarkkaile erottimien pintoja
- Säilytä yksikössä ylipaine suurissa vuototilanteissa, jottei järjestelmään pääsisi ilmaa

Figure 17. Emergency checklist in production line 4, Porvoo (Neste Oyj, 2012)

Figure 18 presents an emergency checklist template that is planned to be used across the whole Porvoo refinery. The idea has been to use application called OhjeNET to create a system where the checklists could be uploaded to devices in the control room as well as to hand held field devices that the field operators would be carrying in the future (and to any other computer based devices). OhjeNET is a system that may be used to create a physical checklists as well. This procedure template is not only a template, but a whole procedure system designed for creating the checklist procedures (emergency, planning, turnarounds and so forth). The system takes concern for creating the checklists, updating the checklists, evaluation of possible hazards, approving the checklist, change requirements, commenting and many other aspects that are required to create valid procedures.

OhjeNET template uses color coding to separate different segments in the checklist. Each segment is colored with segment specific color. On the example emergency checklist of hydrogen plant nr. 1 there are: equipment based procedures, complete interlock which is referring to a steam reformer, methane feed disturbance, CO2 absorber and regeneration disturbance, hydrogen leakage at the absorber, loss of power, loss of instrument air, simple flow charts of the unit and notes how to update the procedures.

Each segment is generally divided to: consequences and actions to be done. The actions to be done may change during the disturbance state of the unit. This has been solved by adding additional titles that are describing the current state of the unit.

Example checklist is designed to be used at the field as well as in the control room. Physical size of this checklist is very small which may bring some challenges in the control room (due dim lightning). The list is rather long and heavy because the same list is designed to be used at the field and in the control room. The font is sans serif, but the letters are leaning on the left and have some curvature in them. The empty space between the lines is not close to recommended 25-33% of overall size of the font but close to 80%. The appearance is quite uniform, but there is still risk that some of the lines are getting more emphasis. The small size and the neutral color of the first page is not optimal for the control room. In addition, there is no designated space for the checklist in the control room. Company's target is to get OhjeNET to field devices and no physical checklists would be necessary. There has been prototypes of RFID equipped physical checklists. The checklist could be checked to see if the checklist is up to date.

Equipment based procedures may become handy at one point. However, it could be recommended to separate these from the emergency checklist on actual oil units. The checklist system is also missing table of contents and navigation system. The color coding is not as handy as QRH's navigation flaps on the right side of the checklist. The checklist is not referring to OQD at any point. OQD could be used after the unit has been stabilized and refers to page numbers or titles could speed up the navigation between these two checklists.

There should be completely different kind of checklist for control room operators. There should be designated spot for the emergency procedures of each unit. The emergency procedure (OQD) should be separated from the unit folder and placed next to the checklist.

This checklist template has many advantages to many other systems: it may be uploaded to computer based systems in the future, the dots are used to separate the items, color coding has been initialized, the main tasks are placed on the list, most of the nice to know information has been removed, is easy to carry at the field, is waterproof and it has been considered that the state of the unit may change. The validation and commenting cycle is being used.

This checklist template has some disadvantages that should be redesigned in the future: the size of it is too small to control room, cover page is very neutral, there are unnecessary coloring in the text (titles for example), the first letter of each line is upper-case character which is not necessary or give any bonus to text, vertical space between the lines is too high, some critical items could be emphasized more (max. temperatures for an example), font should be changed to less playful (the author was informed that this has been changed already in the newer versions), some words that are constantly represented in the text could be used as abbreviations (temperature, pressure and so forth), navigation flaps to right side of the checklist should be introduced, control room checklist should be opened like a book not from bottom to top, the appearance should be more uniform, some additional actions should be introduced and separated clearly from the text to make the list as useful as possible and last the flowcharts could be removed from the emergency checklist if the checklist could be understood without. The template does not guide the designer to create consistent emergency procedures concerning the contents of it.

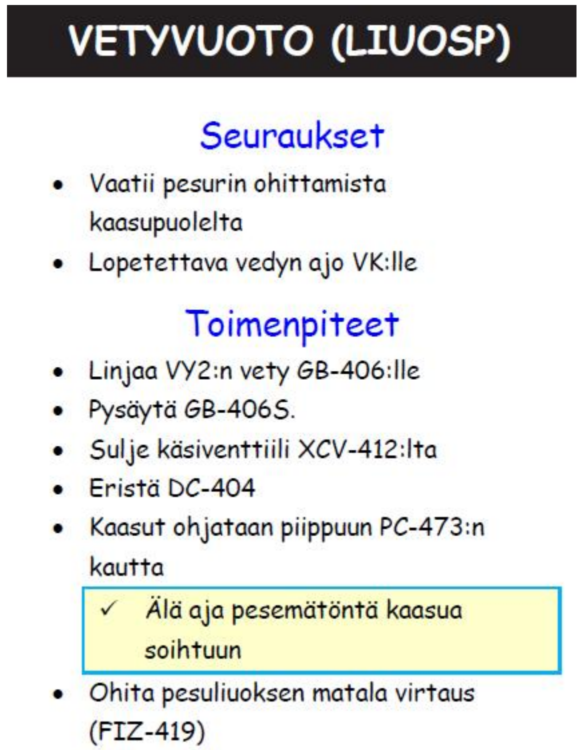


Figure 18. OhjetNET version for hydrogen unit nr. 1 (Neste Oyj, 2013)

9 New template design

As previously mentioned it has been proved that the humans have desire to concentrate on one task at the time. In process industry this may lead to serious consequences. This problematic human factor appeared often during the author's plant visits in Olkiluoto and Loviisa nuclear plants in Finland. This knowledge should be used in favor in oil industry as well because we are fighting against the same problems and it is not possible to change the human behavior in emergency situations. However, it is possible to contribute the operators to make right decisions during process disturbances (process control system, alarm system, procedures, by training, by help from other operators and by proper supervision).

Detailed emergency procedures are good for self-studying, but they are not usable in an emergency situation. After discussing with several shift operators the operators divided into two groups. One group stated that there is not enough time to use these procedures in disturbances and some of them stated that there is already too much documentation available. Another group stated that they have had good experience with these checklists in non-normal operation (Production line 4 control room operators, 2015).

The first group's operators also told that the disturbance situations are always different and there is no one right way to solve the problem. However, some of the first group's operators saw the checklists usable for the younger process operators as well as for the new process units. Operators that were working in the newer process units were clearly more open minded and optimistic for these checklists.

Following the learnings from this research the author was able to design an emergency checklist template for general process units in oil industry. Template follows Gill-Sans MT font in Microsoft Word. The items are placed in time order. The author recommends to use a specific location for the emergency checklists and that they are updated and organized in a professional manner. The pages should be marked with small flaps with corresponding failure and to color code each failure so it would be easy for the operator to open the correct page.

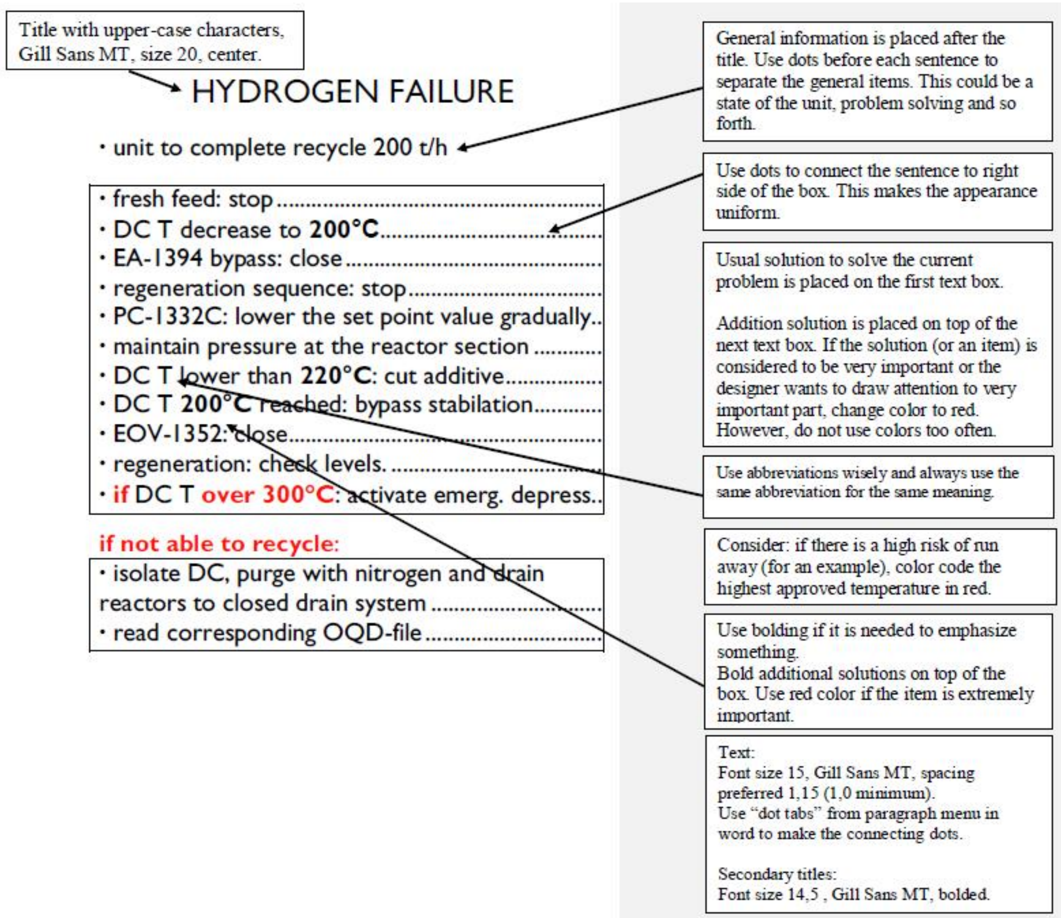


Figure 19. Recommended quick reference guide template

In Figure 19 is the recommended quick reference guide template. Every company should be careful with the abbreviations and make sure that the personnel are trained in advance to minimize the risk of misunderstandings.

The font size should be designed for persons over 50 years old to make sure the font size is sufficient.

FEED FAILURE

· unit to complete recycle 200 t/h

if not able to recycle:

· ESD1321 activates: DC feed bypass ....
· regeneration sequence: stop ....
· H_2 feed: maximize ....
· decrease steam to DA-1327 bottom reboiler ..
· start DC cooling towards **50°C** with H_2 ....
· DC T **lower than 220°C**: cut additive ....
· **50°C** DC T with H_2: maintain ....
· DA-1327 re-boiler: cut steam ....
· **if** DC T **over 300°C**: activate emerg. depress..

if the problem lasts:

· stop H_2 feed, isolate DC, purge with nitrogen and drain reactors to closed drain system ....
· read corresponding OQD-file ....

continues on the next page →

Place each failure to its own page.

If the failure is too long for one page: state clearly that the same list will continue on the next page.

If designing a book-type checklist: use size A5, minimize the margins and consider using color coding for each type of failure (5mm of the right side is in coded for each separate failure).

Before release: check which items could be removed in order to shorten the checklist. If required, refer to operational manual (include number and page number)

Consider using small flaps on the right side of the checklist. Each flap should not be placed on top of each other. Print failure name to the flap so it is easy to see which page to open. Use QRH from aviation as an example.

Figure 20. New template design

It is recommended to use separate pages for each disturbance. If the disturbance/equipment failure takes place on more than one page notify the reader clearly that the same failure continues on the next page.

Try to avoid too many abbreviations, too much bolding and colors. However, the designer may and should presume that the reader has skills to control the unit and is experienced enough to work without the checklist as well. Only add key points to checklists. Avoid long sentences or technical data in the checklists.

This design may be used for book-style checklists as well as folder-type and flap-type checklists. Flap-type is a checklist which is attached to one physical location. Each failure is under a transparent plastic cover. Advantage is that the checklist will be located always at the same location. Book-style checklist is mobile and may be used right next to the keyboard which may be useful in a hectic situations. The best way would presumably be to have both book- and flap-style emergency checklists.

10 Conclusion

The Porvoo refinery's preparedness against major disturbances is at a good level. There are some minor procedures missing or outdated. Process control systems are in good order, except for the alarm systems. Especially in Honeywell DCS systems there is alarm flooding at an unacceptable level. The checklists are still a fairly new subject in the Porvoo refinery, and it is something to improve in the future. Emergency procedures that are affecting the whole refinery are spread around the OQD-system, they should be visible in one location in the company's intranet.

It is likely that the attitude against checklists could change over time if proper lists would be available. The author noticed that the operators were not familiar with aviation-type checklists, and there was a clear distinction between experienced and younger operators. Experienced operators were more likely to be prejudiced and pessimistic towards the checklists. However, the experienced operators were increasingly receiving when they were told that these checklists are only to be used if found necessary and that the use of these lists is not mandatory. It is also evident that the checklist has to be very well written.

It is also good to mention that during writing this research, the author noticed that there are wide range of documentaries and texts of previously happened process emergencies available in English. Unfortunately, there is a lack of material available in Finnish. It could be instructive to translate some document videos into Finnish.

Checklists should not be used to maintain discipline. Management may be tempted to provide checklists that include all the possible information to maintain discipline and to clear out responsibilities, but this is very hazardous to process safety. Too detailed checklists are unpleasant to read, challenging to use and they are not serving their purpose (to maintain control of process). All the personnel designing emergency checklists should be aware of this.

There is a large number of unofficial templates and procedures available in Neste. The number of procedures is increasing, but there is not enough consistency or any system to tell people which procedures are up to date and which are not. Actions against this should be taken immediately.

The hardest part of this research was to be neutral because the subject seems to be very emotional. The author presumes that the recommended template will not be used in practice but hopes that the future designers would try to use some of its features. In Neste, the template could be used in OhjeNET-system in the future. In that case, the OhjeNET-system should be improved further. Current Ohjenet-version is rather beta-version than actual official procedure creation system. The software needs to be designed further.

Based on this thesis the author recommends Neste to improve the quality of the documentation, especially the emergency procedures. Neste seems to have vast amount of projects ongoing but it seems that the projects are cancelled one by one before the goal is reached, and at the same time new projects are being started.

Based on the systematic approach to this subject, the author recommends Neste to create a plan to bring the emergency procedures up to date. Current emergency procedure system that includes many unofficial procedure templates on the side, is not optimal. The company should have uniform line for creating these templates. In addition, company's brand should not play a role in emergency procedures (logos, colors or any other features).

Sources

Albemarle Catalyst Academy, ca. 2010, Catalyst Regeneration & Reactivation. s.l. s.n.

Arimo, E., 2012, (Internal document) Automaatiojärjestelmät. Porvoo: Neste Oyj

Arimo, E., 2015, Automaatiojärjestelmät. [e-mail] (Personal communication, 5 October 2015).

Brady, C., 2015, The Boeing 737 Tehcnical Guide. 71th ed. Cheshire: Tech Pilot Services Ltd

Degani, A., 1992, On the Typography of Flight-Deck Documentation. San Jose: NASA

Degani, A., Wiener E., 1990, Human factors of Flight-Deck Checklists: The Normal Checklist. Ames: NASA

EEMUA, 2015, What we do. [online]. Available at: https://www.eemua.org/tni/About-EEMUA/What-we-do.aspx

Hartley J., 1981, Eighty Ways of Improving Instructional Text. s.l. s.n.

Hiltunen, J., 2015, Aircraft information. [e-mail] (Personal communication, 21 May 2015).

Honkimaa, S., Ranta, E., 2011, (Internal document) Process unit procedures and unit folders. Porvoo: Neste Oyj

Hujanen, T., 2013, (Internal document) Creation and management of management system documents. Porvoo: Neste Oyj

Hujanen, T., 2015, Procedure system of Neste Oyj. [e-mail] (Personal communication, 1 July 2015)

Hydrocarbon Publishing Company, 2013, Refinery Power Failures. [pdf] Available at: http://www.qualitrolcorp.com/uploadedFiles/Siteroot/Industry_Solutions/Refinery%20Power%20Failures%20-%20Causes%20Costs%20and%20Solutions.pdf

Häkkinen, H., 2015, TVO Olkiluoto nuclear power plant's procedure system and simulator room visit. [Conversation] (Personal communication, 20 October 2015)

IEC, 2003, Safety Instrumentated Systems. [pdf] Available at: https://webstore.iec.ch/preview/info_iec61511-1%7Bed1.0%7Den.pdf

IEC, 2010, Functional Safety of Electrical/Programmable electronic safety-related systems. [pdf] IEC 61508. Available at: http://www.iec.ch/functionalsafety/standards/page2.htm

Järvinen, M., 2015, Power grid in Porvoo. [conversation] (Personal communication, 26 September 2015).

Kirkinen, A.P., 2015, Fortum Loviisa nuclear power plant's procedure system. [conversation] (Personal communication, 21 October 2015).

Koski, P., 2015, Process disruptions in gasoline isomerization unit. [conversation] (Personal communication, 2 September 2015).

Kuuluvainen, V., 2015, Automation system in Porvoo. [conversation] (Personal communication, 5 September 2015).

Neerincx, M.A., 2003, Cognitive Task Load Analysis. Soesterberg: Lawrence Erlbaum Associates.

Neste Jacobs, 2013, CR1251 (Internal document). Porvoo: Neste Jacobs

Neste Oyj, 2013, (Internal document) Suojausten koulutusmateriaali. Porvoo: Neste Oyj

Neste Oyj, 2013, (Internal document) MetsoDNA_koulutus. Porvoo: Neste Oyj

Neste Oyj, 2015, (Internal document) Prosessipalojen sammuttaminen OQD-6641. Porvoo: Neste Oyj

Niemilä, J., 2015, Process disruptions in gasoline isomerization unit. [conversation] (Personal communication, 2 September 2015).

Petroleum Development Oman, 2013, Contingency Plan Volume III. [pdf] Available at: http://www.pdo.co.om/hsems/Documents/Procedures/PR-1301%20Emergency%20Procedures%20part%20III%20Contingency%20Plans,%20vol%20II%20Pesonnel%20Centre.pdf

Philips, R. J., 1979, Why is lower-case better? [pdf]. Available at: http://richardphillips.org.uk/maps/map1979.pdf

Production line 1 operators, 2015, Handling the process disruptions in Porvoo refinery [conversation] (Personal communication, 2 September 2015).

Production line 4 control room operators, 2015, Handling the process disruptions in Porvoo refinery [conversation] (Personal communication, 2 September 2015).

Riihelä, T., 2015, Fortum Loviisa nuclear power plant's procedure system. [conversation] (Personal communication, 21 October 2015).

Sihvonen, J., 2015, Emergency power in Porvoo refinery. [conversation] (Personal communication, 28 September 2015).

Appendix 1. SIS logics in process units in Porvoo refinery

Appendix 2. Recommended improvements to Neste

- Procedures generally are well stored and updated. This level should be kept.
- As seen on the Figure 12 some of the updated text in the OQD is in yellow. This is Neste's fashion to inform the reader that a new information has been initialized to the procedure. This is not recommended fashion; hence the text becomes challenging to read, especially if one in a hurry. This system should be developed.
- Some parts of the utility system does not have emergency procedures yet (nitrogen and coolant system in production line 1 for an example). These procedures should be provided to operators.
- Emergency procedures considering the whole refinery should be placed to one location. Currently the files are spread over the intranet and it is challenging to find all the procedures.
- All the new process units should be equipped with emergency checklists (before initial start-up).
- All the high risk units should be equipped with emergency checklists in some time span.
- Alarm rates in major emergencies should be decreased to fractions from the current situation, especially on Honeywells.
- Timer based alarm mute should be considered carefully. Currently the alarm sound is continuous in unit disturbances which only causes stress to operators.
- Alarm pages could be redesigned in the future. It should be considered if the super critical alarms would be presented on the bottom of the page or their block size would be larger to emphasize their importance.
- Checklists should be made official documents and added to official OQD-system that have to be updated periodically (attachments to OQDs).

- Checklist should be considered as a tool, not as a dumping site to increase discipline.

- It would be instructive to have documentaries with Finnish subtitles of past process disasters.

- Simple, practical toolboxes with your own team could be instructive once in a while.

- Checklists for start-ups and shutdowns should be done for each unit. In TA2015 there were some kind of checklists, but they were spread around the procedures which made them impractical to follow. It could be better to make these checklists to block charts to make the parallel items available. Loviisa nuclear power plant used this kind of system and it helped them to organize the right actions on right time. Text-type lists are missing option to make some actions in parallel. Parallel actions have to be performed before moving forward.

- Co-operation with other companies could improve the quality of the documentation crucially.

- Updating of the PIDs should be improved. It should be rethought if the plant engineers would be allowed to make small changes to PIDs (add valve for an example) to fasten the process. It is not justified to say that this could cause safety hazards because the slow updating process is causing even higher hazards.

- There should be a risk assessment about uploading any information from the OhjeNET application to any process control systems (if planned to do so).

- OhjeNET could be developed further to meet lessons of this research.

- Neste should not require brand colors and text types to emergency procedures. This is hazardous to process safety!

- If the hand held field computers are introduced they should be completely water proof and the PMS should be available at the field. If the field operators could see the PMS at the field, it could have unexpected benefits.

Appendix 3. BESSI emergency checklist with new template design